Universidad de Alcalá

LA CIBERDELINCUENCIA

THE CYBERCRIME

Máster Universitario en

Acceso a la Profesión de Abogado

Presentado por:

Dª NURIA FERNANDA CORDERO RUIZ

Dirigido por:

Dr. D. ESTEBAN MESTRE DELGADO

Alcalá de Henares, a 22 de marzo de 2021

INDICE

Página

RESUMEN

Los delitos tradicionales han evolucionado y cambiado su forma de comisión con la aparición de las nuevas tecnologías. El fenómeno de Internet y el uso de las TIC ha repercutido en la vida cotidiana y profesional de las personas físicas y jurídicas. Son varias las ventajas que tienen las TIC, sin embargo, un mal manejo de estas puede acarrear consecuencias jurídicas. En este trabajo se analizan los orígenes de los ciberdelitos, sus características y tipificación. Se estudian los instrumentos jurídicos que han permitido regularlos. Por otro lado, los métodos de investigación tradicionales no son suficientes, teniendo que crearse nuevas figuras, como el agente encubierto informático. Asimismo, se examina la prueba informática, como pieza compleja dentro del proceso penal.

PALABRAS CLAVE: Agente encubierto informático. Ciberdelincuencia. Ciberdelitos. Delitos informáticos, TIC.

ABSTRACT

Tradicional crimes have evolved and changed their shape of commission with the appearance of new technologies. The phenomenon of Internet and the use of ICTs have impacted the daily and profesional life of the natural and legal people. There are several advantages that the ICTs have, however, a bad handling of these can generate legal consequences. In this Project, the origins of Cyber-crime, their characteristics and typification's will be analysed, and at the same time the legal instruments that have permitted to regulate them, will be studied. On the other hand, the traditional methods of investigation are not sufficient, having to create new figures like the computerised undercover agent. Likewise, I will examine the IT proof, as a complex piece inside of the penal process.

KEYWORDS: Computer-related crime. Computerised undercover agent. Cyber-crime. Cybercrimes. ICT.

ABREVIATURAS UTILIZADAS

Art: Artículo

CE: Constitución Española

CERT: Equipo de respuesta a Ciberincidentes en infraestructuras críticas y estrategias

CNP: Cuerpo Nacional de Policía

CNPIC: Centro Nacional para la Protección de las Infraestructuras Críticas y Estratégicas

CP: Código Penal

DNS: Domain Name System

FYCS: Fuerzas y Cuerpos de Seguridad

GDT: Grupo de Delitos Telemáticos

ICT: Information and communication technologies

INCIBE: Instituto Nacional de Ciberseguridad en España

LAJ: Letrado de la Administración de Justicia

LECRIM: Ley de Enjuiciamiento Criminal

LOFCS: Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad

LOPD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales

OCDE: Organización para la Cooperación y el Desarrollo Económico

OEA: Organización de los Estados Americanos

OTAN: Organización del Tratado del Atlántico Norte

Pág: Página

RGPP: Reglamento General de Protección de Datos

Ss: Siguientes

STC: Sentencia del Tribunal Constitucional

STS: Sentencia del Tribunal Supremo

TIC: Tecnologías de la Información y Comunicación

TS: Tribunal Supremo

UE: Unión Europea

UIT: Unión Internacional de Telecomunicaciones

UNED: Universidad Nacional de Educación a Distancia

UNODC: Oficina de Naciones Unidad contra la Droga y el Delito

WWW: World Wide Web

INTRODUCCIÓN

Los ciberdelitos no son recientes. Así se muestra en el primer capítulo de este trabajo, donde abordamos el origen de los mismos, y mostramos sus diferentes etapas, su evolución hasta convertirse en lo que son hoy: una modalidad dentro de la esfera jurídico penal, que engloba varios tipos de delitos. Podemos observar que al principio se denominaban delito informático; sin embargo, este concepto quedó atrás y fue sustituido por el actual, con motivo de la aparición de la red de Internet. Ya no se consideraba delito solo la conducta de dañar un dispositivo electrónico, sino también la conducta de causar un daño a través de Internet.

En el primer capítulo del trabajo abordamos también las notas características de las TIC y de la ciberdelincuencia. Podrá parecer que hablamos de lo mismo, no obstante, las características de las TIC son las que han favorecido la aparición de la ciberdelincuencia. El surgimiento de Internet, como adelantábamos, es un arma de doble filo; por una parte, ha provocado que nos encontremos conectados en todo momento, permitiendo recibir y enviar cualquier tipo de información en un breve periodo de tiempo, pero, por otro lado, un mal manejo de esta herramienta y de los dispositivos electrónicos puede conllevar consecuencias jurídicas. Las ventajas que tienen las TIC (masividad, celeridad y anonimato) son a su vez, paradójicamente, las desventajas de utilizar Internet. Mejor dicho, de un uso incorrecto de Internet. Observaremos las características de la ciberdelincuencia, que se nutren de las ventajas de las TIC, y que han dado lugar, sin quererlo ni buscarlo, a que los ciberdelincuentes vean nuevas oportunidades para delinquir.

Esas ventajas de las que hablaremos han favorecido la aparición de nuevos delitos, más bien una transformación en el modo de comisión de los delitos tradicionales. Siguiendo esta línea, analizaremos con posterioridad la regulación de la ciberdelincuencia, tanto desde una óptica nacional como internacional, haciendo alusión al Convenio de Budapest, instrumento jurídico clave en la lucha contra la ciberdelincuencia. Igualmente, estudiaremos la regulación y medios de prevención contra aquella en España.

Asimismo, analizaremos la clasificación delictual de los ciberdelitos, agrupándolos según el bien jurídico lesionado. En cada uno, explicaremos brevemente la conducta típica y antijurídica, y las penas que impone nuestro Código Penal.

El hecho de que surjan nuevas formas de comisión de los delitos tradicionales que conocemos arroja también la necesidad de contar con nuevas modalidades de investigación criminal. En este sentido, nos encontramos con una figura que ha adquirido importancia en los últimos años, dada su utilidad para la investigación de diversos ciberdelitos, entre ellos el child-grooming, la pornografía infantil o el ciberterrorismo. El agente encubierto conocido en Derecho Penal va un paso más allá con motivo de la repercusión de los ciberdelitos, creando una modalidad: el agente encubierto informático, figura que solo tiene cabida dentro del marco de la ciberdelincuencia y revestido de unas peculiaridades que hacen de él una figura significativa para luchar contra los delitos cometidos por organizaciones criminales.

Tras analizar el origen, las características, la regulación y las clases de ciberdelitos, y una de las herramientas de investigación en el proceso penal, el agente encubierto informático, finalizaremos con el estudio de la prueba informática, peculiar en tanto en cuanto que se caracteriza por sus requisitos de admisibilidad. De igual forma, explicamos la problemática que existe a la hora de practicar dicha prueba, teniéndonos que valer de herramientas ofimáticas y programas fiables y con garantías para dar seguridad jurídica y validez a la prueba que se pretende presentar, e inclusive, hablaremos de quién o qué medios pueden dar validez a la misma.

CAPITULO PRIMERO

CONSIDERACIONES GENERALES SOBRE LOS CIBERDELITOS

1. Evolución histórica de los ciberdelitos

Los ciberdelitos se encuentran muy presentes en nuestro panorama social, causando un gran impacto jurídico y económico. El término que se utiliza para referirse a esta nueva modalidad delictiva ha sido acuñado con el paso de los tiempos, pasando de

ser considerados como delitos informáticos a ser la categoría dentro de la que encajan ahora estos tipos de delitos.

Es imposible conocer cuál fue el primer ciberdelito que se cometió, dado que el ciberdelito no es una manifestación reciente, pues hace varios años que surgió. En el siglo XX, el concepto de delincuencia sufre una transformación motivada por la evolución social y los procesos de adaptación del ser humano promovidos por la aparición de las tecnologías. No obstante, sí es posible estudiar la causa de su origen y cómo era en sus inicios, así como qué factores o herramientas facilitaron su expansión y evolución. En este punto abordaremos qué hechos favorecieron su surgimiento y los factores que incidieron en su evolución.

La historia del ciberdelito se diferencia en cuatro etapas:

1) Etapa de germinación.

2) Etapa de desarrollo.

3) Etapa de expansión.

4) Etapa de rutinización.

Los ciberdelitos surgen poco después de la creación de los primeros ordenadores. Siguiendo esta línea, la primera etapa de los ciberdelitos abarca desde 1940 hasta 1960. En aquel entonces, los consumidores prestaban más atención a las características y ventajas que ofrecían los ordenadores que al grado de fiabilidad respecto a cuan protegido se encontraban en el momento de su uso o si los propios sistemas estaban protegidos, así como los datos que se almacenaban en ellos. Estados Unidos fue de los primeros países donde se asentó un precedente, debido al caso de un empleado de un banco que utilizó el ordenador de la propia entidad para malversar en operaciones en las cuentas a largo plazo. Sin embargo, en aquella época los ordenamientos no contemplaban aún una regulación para estos supuestos.

Entre los años 1970 y 1980 tuvo lugar la segunda etapa. En ella aumentó la dependencia de los ordenadores en las personas e instituciones públicas y privadas y, por ende, aumentaron las amenazas por parte de los ciberdelincuentes, donde vieron una oportunidad. Esa dependencia se debió al desarrollo tecnológico, que causó una revolución de la información, pudiendo compartirse de forma instantánea y económica, pero, pese a esas ventajas que proporcionaban, continuaron siendo vulnerables a la

manipulación criminal, por tanto, esa información que a través de los ordenadores era posible transmitir fue empañada por la vulnerabilidad de los dispositivos y sus sistemas operativos, de la que se aprovecharon los primeros ciberdelincuentes.

En la década de los setenta del siglo XX se cometieron fraude económico, manipulación de datos, espionajes empresariales, etc. En este sentido, Hernández Díaz señala que "la difusión de ordenadores en el mundo empresarial supuso que la gran parte de delincuencia informática tuviese relación con la delincuencia económica, hasta el punto en que esas nuevas modalidades de delincuencia económica eran las que integraban el concepto de delito informático o las principales manifestaciones del mismo"[1].

En los años ochenta de ese siglo, con el uso personal de ordenadores, aumentó el número de delitos informáticos. Fue en aquella época cuando surge la piratería del software, afectando al derecho de propiedad intelectual, que más adelante, a finales de los años noventa, se extendería a otros productos, como música o películas. Fue precisamente en esa década de los ochenta cuando se consideró como abuso utilizar el ordenador personal de otro individuo sin su consentimiento. Esto que en un principio no tenía importancia, debido a que la disponibilidad de ordenadores era insuficiente y no había otra solución que utilizar varias personas un mismo dispositivo, con el tiempo adquiere relevancia, pues la disponibilidad era mayor y se hizo innecesario que los usuarios se entrometieran en los sistemas de otros.

Al tratarse de una nueva modalidad de delito, las autoridades reaccionaron de una forma paulatina. El desarrollo de la tecnología informática tuvo un doble filo: por un lado, fue diseñada para mejorar el bienestar social, pero, por otro lado, constituyó una fuente importante de amenazas para el orden social; asimismo los incidentes de seguridad informática aumentaron constantemente.

En la tercera etapa, que duró toda la década de 1990, los ordenadores personales estaban en hogares y oficinas, con ello los ciberdelitos habían entrado en un rápido proceso de globalización favorecido con la aparición de la *World Wide Web* (WWW), produciéndose un fuerte cambio en la comisión de los delitos informáticos, pues esta interfaz gráfica permitía compartir información desde cualquier parte del mundo, enviando y recibiendo por tanto información, creando un entorno digital. Además, trajo

[1] Hernández Díaz, L.," El delito informático", Eguzkilore, núm. 23, San Sebastián, diciembre de 2009, pág. 229.

consigo el surgimiento de una nueva forma de difusión de contenidos ilegales, como por ejemplo pornografía infantil o discursos racistas o de odio. En esta línea, Hernández Diaz señala que "justamente son este tipo de conductas vinculadas a la difusión de contenidos ilícitos las que se pueden aprovechar de la enorme implantación que tiene WWW a nivel mundial, y de las características que dificultan su descubrimiento, persecución y prueba"[2]. Los usuarios que accedían a Internet se enfrentaron a amenazas dentro de un ciber espacio globalizado. La información personal podía ser atrapada durante el proceso de su transmisión, es decir, atacada durante la navegación voluntaria en Internet. Asimismo, las páginas webs dejaron de ser únicamente herramientas mediante las cuales se realizaban los ataques para convertirse también en el objetivo de estos. Se aprovecharon las comunicaciones electrónicas, concretamente del correo electrónico, utilizándolo como medio publicitario para un marketing clandestino y se produjeron ataques de programas maliciosos. En consecuencia, los negocios de antivirus y de servicios de seguridad continuaron desarrollándose.

La cuarta etapa se desenvolvió a partir del año 2000, cuando los ciberdelitos se generalizaron y convirtieron en una rutina para los delincuentes. En este período se consolida la dependencia que tienen los gobiernos y organizaciones internacionales de los sistemas informáticos, utilizados tanto para un mejor funcionamiento como para el almacenamiento de datos relevantes o secretos. Ello produjo que los ciberdelincuentes vieran una oportunidad para la comisión de delitos que atentasen contra la seguridad del Estado y ataques terroristas a través de Internet.

A raíz de aquella aparición, en el siglo XXI se consolida ese entorno digital y pasa a formar parte del día a día de las personas. Según Fanjul, "la nueva era digital propicia el nacimiento de nuevas formas de delito: el ciberdelito"[3]. En este sentido, afirma que "el ciberdelito es una forma de delito consecuencia de la evolución tecnológica"[4].

Esta novedad fue una oportunidad de mercado para los delincuentes. En principio, los ciberdelincuentes se unieron a organizaciones criminales que operaban fuera de los medios virtuales, de forma que los primeros aportaban el conocimiento y los segundos la experiencia. Sin embargo, con el tiempo son las bandas organizadas quienes compran los servicios a ciberdelincuentes, resultando estos últimos cooperadores necesarios,

[2] Ibidem, pág. 230.
[3] Fanjul, M.L, "Conceptualización, evolución y clasificación del ciberdelito empresarial", AMEC Ediciones, Madrid, 2018, págs. 43-44.
[4] Ibidem, pág. 47.

equiparándose en el Derecho español como autores del hecho pese a que únicamente tengan consideración de instrumento para realizar el hecho delictivo, debido a que sin su intervención en la ejecución no se hubiera desarrollado. Por otro lado, la acumulación de datos de carácter personal por parte del gobierno hace que se replantee crear métodos que aseguren el carácter reservado de esos datos, naciendo así el concepto de *privacity* que engloba la acumulación de información de los individuos y el uso que se hace de ella en bases de datos.

Hoy por hoy, casi cualquier delito puede cometerse por medios electrónicos, no todos, pues es imprescindible que en la ejecución del delito tengan cabida las TIC como medio de comisión u objeto del mismo.

2. Concepto y notas características

Con la llegada de las TIC se ha producido una gran incertidumbre sobre el tratamiento de los datos que compartimos e intercambiamos a través de ellas. Dada esa inquietud, varios países han introducido en sus ordenamientos jurídicos protocolos y políticas de seguridad en aras a controlar el flujo de información en internet. Esas normas jurídicas van dirigidas a proteger los derechos e intereses del sector público como aquellos derechos fundamentales que gozan los ciudadanos. Las tecnologías han ido evolucionando a la par que la sociedad, por ello es importante desarrollar programas o métodos que ayuden a paliar esta nueva forma de delincuencia, cuya característica principal es su operación a través de la red.

Para comprender los tipos de ciberdelitos que se dan en la actualidad, es necesario partir en primer lugar del concepto de ciberdelito. Son varios los autores que lo han abordado; no obstante, es una tarea ardua proporcionar una sola definición del concepto pues, aunque en su mayoría están de acuerdo en que es una nueva forma o modalidad de comisión delictiva, algunos autores hacen precisiones sobre los elementos que deben darse para que sea un ciberdelito como tal, pues no siempre se trata de delitos que se cometen a través de dispositivos electrónicos, sino que además dañan dichos dispositivos, siendo objeto de ese delito.

En un primer momento, se entendió por delito informático aquella acción antijurídica realizada mediante dispositivos electrónicos con la finalidad de dañar otros equipos o provocando un daño en sí mismo. Sin embargo, con la aparición de Internet, se

produjo una evolución tanto en la forma de cometer el delito como en el término. Varios delitos se cometían a través de las tecnologías e Internet, por lo que delito informático se convirtió en un tipo de delito dentro del ciberdelito (un tipo dentro de una modalidad) y este término abarcaría toda acción típica y antijurídica cuya comisión se realice o esté favorecida por el empleo de las TIC, pues el delito se comete mediante estas. Siguiendo esta línea, Miró Llinares comenta que la denominación de delitos informáticos se ha sustituido por la de cibercrimen y cibercriminalidad, que provienen del término anglosajón "cybercrime", una palabra compuesta por *cyber*, derivado del término cyberspace, y el término *crime*, concepto que sirve para englobar la delincuencia dentro del ciberespacio. El ciberdelito, en un principio, se caracterizó porque se cometía a través de los ordenadores, sin embargo, con el surgimiento de Internet, los delitos tradicionales se cometen empleando ordenadores y a través de Internet. Hoy en día se caracterizan por encontrarse completamente determinados por el uso de Internet y las TIC. Esto se traduce en que ya no se utilizan exclusivamente los medios electrónicos para delinquir, sino que además Internet se convierte en una oportunidad para la comisión de infracciones tradicionales, de forma que los ciberdelitos quedan determinados por los medios electrónicos y por Internet[5].

En palabras de Urbano Castrillo, el ciberdelito es un "tipo de delito, tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta. El convenio de Budapest ofrece un concepto basado tanto en la utilización de determinadas técnicas y modos de proceder informáticos […] como en ciertos contenidos cuya vulneración se ve facilitado por el medio Internet"[6].

Por tanto, en definitiva, el delito informático sería un tipo dentro de los ciberdelitos y estos a su vez una modalidad de delito dentro del ámbito del Derecho Penal.

Tal como expresa Espinosa Sánchez, son "aquellos actos ilícitos que, valiéndose de las ventajas surgidas de la revolución tecnológica, consiguen penetrar en las defensas de los sistemas informáticos, provocando la vulneración de éstos, y dando lugar a una pluralidad de delitos que pueden variar en su esencia delictiva"[7].

[5] Miró Llinares, F.: "El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio", Marcial Pons, Madrid, 2013, págs. 37-38.
[6] De Urbano Castrillo, E.: "Los delitos informáticos tras la reforma del CP de 2010", Revista Aranzadi Doctrinal, núm. 6, octubre, 2011, pág. 18.
[7] Espinosa Sánchez, J.F.: "Ciberdelincuencia. Aproximación criminológica de los delitos en la red", La Razón Histórica, núm. 44, septiembre-diciembre, 2019, pág. 155.

Por tanto, podemos definir ciberdelito como aquella acción típica y antijuridica que es cometida a través de las TIC, atentando a la disponibilidad, integridad y confidencialidad de los sistemas informáticos, de las redes, de los datos y derechos de terceros, o haciendo un uso fraudulento de ellos. El ciberdelito se ve favorecido por las TIC, pudiendo emplearse como medio para la comisión u objeto sobre el que actúa.

En este sentido, encontramos la definición más certera de ciberdelito por parte de Gómez Hernández y Rayón Ballesteros, que lo definen como "cualquier infracción punible […] en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito"[8].

El fin que persigue la ciberdelincuencia es el ataque a los dispositivos informáticos, a los datos almacenados y a la información informatizada.

Así es cómo los ciberdelitos, si bien no son una novedad para la sociedad, sí lo son en el plano jurídico, concretamente para el Derecho penal, rama que se ha dedicado a estudiar a fondo sus elementos y características, así como los desafíos que han traído consigo los mismos. Siguiendo en esta línea, abordaremos las principales notas características de los ciberdelitos.

A lo largo de la historia, el delito ha encontrado un aliado en la tecnología, debido a que los delincuentes han buscado innovar utilizando herramientas y tecnología para alcanzar sus objetivos[9] .

Entre los aspectos positivos de estas nuevas tecnologías destacan, entre otras, la posibilidad de comunicación instantánea, la eliminación de fronteras para la comunicación que ha llevado a desdibujar cualquier distancia, la posibilidad de teletrabajo, etc. Entre todas esas características que tienen las nuevas tecnologías, nos centraremos en tres que desde nuestro punto de vista son las más relevantes:

1. Inmediatez.
2. Anonimato.
3. Masividad.

[8] Gómez Hernández, J.A y Rayón Ballesteros. M.C: "Cibercrimen: particularidades en su investigación y enjuiciamiento", en "Anuario jurídico y económico escurialense", núm.47, 2014, pág. 211.
[9] Cerezo Domínguez, A.I: "La ciberdelincuencia en España: un estudio basado en las estadísticas policiales", Revista electrónica de estudios penales y de la seguridad, núm. 6, abril, 2020, págs. 2-3.

Estas características, combinadas con otros factores de los que hablaremos más adelante, son los cimientos para generar el efecto potenciador del delito. Es decir, los ciberdelincuentes aprovechan las características de las TIC para realizar el delito, puesto que su comisión mediante estas o sobre ellas tiene un mayor beneficio que su comisión de la forma tradicional.

Muchos delitos clásicos, como la estafa, el acoso sexual, o la pornografía infantil, ya se hallaban antes que existiera Internet. Es a través de dispositivos telemáticos cómo desde cualquier lugar con conexión a Internet (a distancia), el delincuente puede atacar a la vez un bien jurídico protegido, como pudiera ser la intimidad o el secreto de comunicaciones, de forma masiva e instantánea y en función del conocimiento que tenga el delincuente, puede utilizar herramientas o mecanismos que dificulten su identificación o rastreo, facilitando mantener su anonimato.

Por ende, los ciberdelitos presentan las siguientes características:

1. Anonimato. Nos referimos al desconocimiento de la identidad del delincuente. Este puede alcanzar distintos niveles de anonimato con las tecnologías. La identidad real del delincuente puede quedar oculta, o bien la conexión desde la cual realiza la acción delictiva. Tener conocimientos en la materia y habilidades necesarias permite al ciberdelincuente, además de cometerlo, poder encubrirlo. El anonimato conlleva a su vez una difícil persecución del ciberdelito, pues, al desconocer en muchas ocasiones quién es el autor real o desde qué red ha cometido el delito, no es posible condenar el hecho, quedando impune.

2. Inexistencia de barreras geográficas. Una de las características de las TIC es permitir que la comunicación sea en el momento. No se encuentran fronteras geográficas que impidan que la comunicación se mantenga a distancia, viajando la información y el contenido de un país a otro. Las tecnologías permiten la comunicación a distancia a través de las redes; en este sentido, el ciberdelincuente puede encontrarse físicamente alejado de la víctima, inclusive en otro país, siendo lo más usual, dado que en varios estados se encuentra una escasa o nula regulación sobre esta materia, así como una falta de cooperación judicial internacional, convirtiéndose estos estados en paraísos cibernéticos, aquellos lugares donde es más fácil la comisión de los ciberdelitos.

Gracias a que las tecnologías permiten una comunicación a distancia, el factor geográfico queda eliminado, traduciéndose este hecho en numerosas ventajas como inconvenientes, como poder cometerse un ciberdelito desde cualquier parte del mundo. En consecuencia, la conducta antijurídica puede realizarse en un determinado país, pero el resultado se produce en otro. Por tanto, el factor geográfico que se ve eliminado o reducido gracias a la existencia de los medios de comunicación telemáticos y sobre todo de Internet, conlleva que el ciberdelito adquiera un carácter transnacional en ocasiones, que deriva en la involucración de varias jurisdicciones, legislaciones, organizaciones de control e investigación, etc.

3. Instantáneos. Esta característica está estrechamente relacionada con las nuevas tecnologías, debido a que el momento de realización del ciberdelito es instantáneo. Los ciberdelitos se cometen con gran celeridad e ipso facto. Es decir, el perfeccionamiento del delito se da en el mismo momento en el que el delincuente lleva a cabo la acción. Es por ello por lo que la celeridad es una característica notoria en los ciberdelitos, pues se emplea poco tiempo en su comisión y el delito se consuma en cuestión de segundos.

4. Masivos. La masividad como característica de las TIC se ve reflejada en los ciberdelitos, dado que estas permiten la difusión masiva de contenidos.

5. Pluriofensivos. Con esta característica nos referimos a que los ciberdelitos pueden afectar a más de un bien jurídico protegido a la vez.

6. Facilidad de comisión. Los ciberdelitos también se caracterizan por la escasez de recursos que se requieren para que el delincuente los cometa. Además de los escasos medios, tampoco se requieren conocimientos avanzados ni una gran experiencia, sino que con tener un dispositivo electrónico al alcance y conexión a la red Internet puede fácilmente realizarse la acción delictiva. Inclusive, cabe la posibilidad de encontrar personas que ofrezcan realizar esos servicios ilícitos, conocidos como empresarios criminales individuales, una forma de crimen

organizado cuyo modelo de negocio se basa en "el crimen como servicio y la internacionalización como reflejo de un mundo globalizado"[10].

CAPITULO SEGUNDO

LA REGULACIÓN DE LA CIBERDELINCUENCIA

1. El Convenio sobre la Ciberdelincuencia o de Budapest

Para combatir esta forma de delincuencia es necesario contar con instrumentos de regulación, así como con personal de investigación especializado y un procedimiento rápido y específico para este tipo de delito.

En este sentido encontramos el Convenio sobre Ciberdelincuencia suscrito en Budapest el 23 de noviembre de 2001, de ahí que se le conozca también por Convenio de Budapest. Dicho Convenio entró en vigor el 1 de julio de 2004. Surgió como respuesta a la necesidad de buscar medios eficaces para luchar contra los ciberdelitos de forma comunitaria y con el objetivo de armonizar, desarrollar y adoptar políticas penales comunes para proteger a la sociedad a partir de una legislación propia nacional y una estrecha cooperación internacional motivada por la falta de fronteras en la comisión del delito. En definitiva, se hizo necesario crear una política penal común que sirviera como modelo a todos los países que se adherían o ratificarían el Convenio, de forma que cada uno con posterioridad desarrollase una legislación propia, de carácter nacional, pero manteniendo una política de cooperación internacional[11].

Por tanto, al tratarse la ciberdelincuencia de un fenómeno transnacional, surgen esfuerzos para conseguir una regulación de aquélla a nivel internacional. El Convenio de Budapest es concebido como una herramienta necesaria para la lucha contra la ciberdelincuencia. Pese a ser un Convenio de carácter europeo, queda abierto a la adhesión por parte de otros estados que no sean miembros del Consejo de Europa, tal

[10] Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave, Boletín Oficial del Estado, núm. 46, de 22 de febrero de 2019.
[11] Gómez Hernández, J.A y Rayón Ballesteros. M.C: "Cibercrimen: particularidades en su investigación y enjuiciamiento", op. cit., página 212.

como establece en su artículo 37. En la actualidad, el Convenio ha sido ratificado por sesenta y cinco Estados, tanto por miembros de la Unión Europea como por Estados no europeos. Asimismo, diversas organizaciones internacionales se han adherido a él, tales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT). El Convenio ha sido firmado por todos los Estados miembros de la UE, pero hoy en día continua sin que sea ratificado por Irlanda y Suecia.

En el Preámbulo del Convenio encontramos el objetivo que persigue con su creación, el cual es "incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos". Para alcanzarlo se hizo necesaria una cooperación internacional reforzada, rápida y eficaz.

De la lectura del Convenio se concluye que su creación se debió a los siguientes motivos[12]:

a) Promover la armonización de las leyes penales sustantivas que regulan las conductas delictivas que tienen lugar en el ámbito de las TIC, es decir, armonizar la legislación que regula la ciberdelincuencia a nivel del derecho penal sustantivo de cada Estado parte del Convenio.

b) Poner en común las reglas de procedimiento penal para la investigación y persecución de las conductas delictivas y mejorar las capacidades nacionales de conformidad al derecho procesal de cada Estado parte.

c) Establecer un régimen ágil y efectivo de cooperación internacional.

El Convenio es el punto de partida de la regulación de la ciberdelincuencia a nivel internacional. Tal como dice Acurio del Pino, este se basa principalmente en conseguir la armonización de las leyes nacionales sustantivas y procesales, de manera que, cuanto mayor sea el alcance penal en cada país, menor será la posibilidad de que los hechos delictivos queden impunes. Rodríguez Bernal explica en su obra[13] que el principio del

[12] Acurio Del Pino. S.: "Delitos informáticos: generalidades", Organización de los Estados Americanos, 2017, págs. 46-48. Visto el día 20/08/20 en la web: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf .

[13] Rodríguez Bernal, A.P.: "Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia", Revista de Derecho Informático, núm.103, septiembre, 2007, pág.13.

Convenio se desarrolló en 1983, cuando un grupo de expertos se reúne y recomienda a la OCDE la necesidad de armonizar las leyes nacionales reguladoras de los delitos informáticos, materializándose esas ideas debatidas en un informe tres años después. Fue a partir de ese momento cuando el Consejo de Europa toma la iniciativa de regular la ciberdelincuencia, y publicó en 1989 la Recomendación N.º 89 (9), que ofrecía a los legisladores nacionales directrices para definir ciertos delitos informáticos, es decir, se mostraba una clara tendencia a incorporar los delitos informáticos en los ordenamientos y regularlos. Esto desembocaría en el Convenio de Budapest, aunque no sería hasta 1997 cuando se iniciarían las negociaciones para elaborar dicho Convenio. Gran parte de su contenido se debe a la puesta en común de respuestas ante el desarrollo de las TIC que tuvo lugar en la segunda cumbre de Jefes de Estado y de Gobierno en Estrasburgo. Sin embargo, no fue hasta el año 2000, tras más de treinta versiones del proyecto, cuando el Consejo de Europa se volcó plenamente en la elaboración final del Convenio. Finalmente, los miembros del comité encargado de la redacción llegaron a un consenso, publicando el Proyecto de Convención sobre el Delito Cibernético, el cual fue aprobado en el año 2001 por el Comité de Ministros. En otra gran parte del contenido del Convenio influyeron las recomendaciones que hizo el Comité de Ministros del Consejo de Europa, así como algunas resoluciones dadas por el Consejo de Ministros de la Unión Europea.

Respecto a la estructura del Convenio, consta de cuarenta y ocho artículos, divididos en cuatro capítulos, que a su vez se fraccionan en secciones y títulos, y un preámbulo.

El primer capítulo hace referencia a la “Terminología”, necesario para entender el contenido del Convenio, definiendo conceptos como: sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico.

El segundo capítulo recoge las “Medidas que deberán adoptarse a nivel nacional”, y a su vez se divide en dos secciones.

Por un lado, distinguimos el Derecho penal sustantivo, donde se establecen los tipos de ciberdelitos:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.

- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Asimismo, recoge elementos de Derecho sustancial, tales como la tentativa y la complicidad, la responsabilidad de las personas jurídicas y las sanciones y medidas respecto a los delitos previstos.

La segunda sección corresponde al Derecho procesal, esto es, el procedimiento, condiciones y medidas de protección, es decir, garantías, obtención y conservación de los datos, registro, etc., y la tercera sección se refiere a la jurisdicción y los criterios para determinarla.

El tercer capítulo se refiere a la cooperación internacional, dividiéndose en principios generales y otros relativos a la extradición, la asistencia mutua y procedimiento a seguir en ausencia de esta o de acuerdos internacionales aplicables, la información entre Estados, el intercambio de datos y el establecimiento de una red 24/7 ("punto de contacto localizable las 24 horas del día, siete días a la semana").

El último capítulo contiene las disposiciones finales que tiene todo Convenio, dedicadas a determinar el acceso de otros países a aquél, es decir, su firma y entrada en vigor, su adhesión al Convenio, su aplicación territorial, los efectos, la forma en la que se hacen las declaraciones, reservas, enmiendas, consultas, denuncias y notificaciones, etc.

Con base en la estructura que sigue el Convenio, podemos diferenciar dos grandes bloques: el primero dedicado al Derecho Penal Internacional, que abarca desde el artículo 2 al 13, y el segundo dedicado al Derecho Procesal Internacional, constituido por los artículos 14 a 35.

Además, dadas las críticas que afirmaban que el Convenio no contemplaba la problemática de actos racistas y xenófobos y la explotación sexual de la infancia en la Red cometidos a través de sistemas informáticos, se elaboró un Protocolo Adicional que tipificaba como delito los actos racistas y xenófobos, abierto a la firma el 28 de enero de 2003, que España ratificó en 2015, y un Convenio para la protección de los niños contra la explotación y el abuso sexual, abierto a la firma en 2007, que entró en vigor en España en 2010, en el que se refleja por primera vez en un Convenio el ciber-acoso, o también denominado *grooming*, que no se regulaba en el Convenio de Budapest.

En conclusión, en el Convenio se tipifican determinadas conductas, consiguiéndose la armonización en el Derecho sustantivo de los Estados parte. Se dejan

abiertas las posibilidades de punición a los Estados parte, lo que se traduce en una aplicación flexible de los tipos. Por tanto, esto permite aunar los criterios para una lucha común, pero respetando el ordenamiento jurídico propio de cada Estado. Bajo expresiones como "cualquier parte podrá exigir" o "cualquier parte podrá reservarse el derecho", se entiende que el Convenio crea un sistema que en principio tratará de garantizar la conciliación con los demás sistemas jurídicos.

2. Regulación jurídica en España

En el Código penal español no se contempla expresamente el concepto de ciberdelito, es decir, no hay precepto donde se defina, puesto que no se trata de un tipo de delito en sí mismo, sino una categoría, por lo que su definición variará dependiendo del delito de que se trate, aunque el denominador común de todos ellos sea la presencia de las TIC. Identificamos los delitos informáticos en el CP como aquellos que se producen por medio de un ordenador o dispositivo electrónico, por ejemplo una tablet, un reloj inteligente o un teléfono móvil con conexión a Internet; siendo el objeto sobre el que recae la conducta el propio sistema, programa o equipo informático, o bien porque ese ordenador o dispositivo es utilizado como medio para realizar la conducta típica, o bien porque lo que se salvaguarda es la integridad, disponibilidad y confidencialidad de la información o los datos[14].

España estuvo presente en el Convenio desde los primeros pasos encaminados a la negociación, debido a su contexto geopolítico. Además, su pertenencia como miembro del Consejo de Europa llevó a firmarlo el mismo día de apertura de la firma, pero no fue hasta el 1 de octubre de 2010 cuando entró en vigor para España, tras su ratificación. Como hemos dicho, no aparece en el CP el concepto "delitos informáticos", pero sí están regulados; de hecho, desde la publicación del Código vigente (en 1995) se dio importancia a estos tipos de conductas. Por tanto, desde el origen del CP fueron previstas varias conductas que constituyen los tipos informáticos. No obstante, cuando se elaboró dicho CP no se contemplaron los posibles cambios que van aparejados a toda evolución social ni la importancia que adquirirían las TIC en la vida cotidiana, lo que llevó más adelante, con el fin de adaptar los tipos a esta nueva realidad, a realizar modificaciones legales en el CP respecto a este tema, reflejadas en la reforma que tuvo lugar en 2015.

[14] Gómez Hernández, J.A y Rayón Ballesteros. M.C: "Cibercrimen: particularidades en su investigación y enjuiciamiento", op. cit., pág. 212.

El acoplamiento del Convenio con el ordenamiento español se produjo correctamente. Respecto a la parte del Derecho Penal sustantivo, los preceptos del CP son similares a los que recoge el Convenio. Y, respecto a la parte de Derecho Procesal Penal del Convenio, no planteó conflictos relevantes. Por ejemplo, de la interpretación de los artículos 16 a 21, relativos a los datos informáticos, en que de manera reiterada se alude a las autoridades competentes como órgano de control de aquellas medidas tendentes a prevenir el delito. Se entiende que estas "autoridades competentes" no generan inconveniente con el ordenamiento jurídico español siempre que se entiendan como obligatoriamente judiciales. Asimismo, las medidas cautelares que se prevén en los artículos 299 y ss. LECrim también están recogidas en el Convenio. Por otro lado, los criterios de atribución de competencia que contempla la Ley Orgánica del Poder Judicial en sus artículos 21 y ss. son idénticos a los recogidos en el Convenio. Lo mismo sucede con el artículo de la extradición, contemplado en los arts. 824 y ss. de la LECrim, y el 24 del Convenio. Por último, en nuestro ordenamiento se contempla lo que el Convenio regula en los artículos 25 a 27 sobre los Principios generales relativos a la asistencia mutua y los artículos 29 a 35 sobre la Asistencia mutua en materia de medidas provisionales. Tampoco generan dudas las cláusulas finales de los artículos 36 y ss. del Convenio[15].

Tal como hemos mencionado, en 2015 se produjeron modificaciones en el CP con relación a los ciberdelitos. Se introdujeron dos nuevos delitos: *sexting* y *stalking.* El primero se encuentra regulado en el apartado siete del art. 197, y el segundo en el art. 172 ter del CP. El concepto de cada una de estas conductas se verá más adelante con mayor detalle; ahora únicamente estudiaremos el motivo de su tipificación. En consonancia con lo anterior, con su tipificación se produce la absorción del desvalor específico de las conductas, que, hasta ese momento, no encontraban su encaje legal, es decir, no había precepto en el CP que previera tales conductas, pues recordemos que, pese a que se contemplaban los delitos informáticos, se partía de un Código penal elaborado hacía veinte años, época en la que aún no existían las redes sociales como WhatsApp, Facebook, Twitter o Instagram y algunos dispositivos electrónicos (smartwatches, móviles, etc.), que se encuentran tan presentes en nuestro día a día. Por ello, al no saber en qué precepto encajaban esas conductas, se dictaron varias sentencias absolutorias por su atipicidad, por

[15] Diaz Gómez. A.: "El delito informático, su problemática y a cooperación internacional como paradigma de su solución: El convenio de Budapest", REDUR n.º 8, diciembre 2010, págs. 197-198.

no encontrarse contempladas en el CP, y, por ende, en aplicación del principio de legalidad, quedando impunes[16].

Por tanto, al contemplar el CP los ciberdelitos, se deja al margen una ley penal especial para ese tipo de delitos. Sin embargo, desde un principio y en las sucesivas reformas no se ha destinado un título a los delitos informáticos o ciberdelitos o una norma común que los regule y establezca las sanciones. La reforma de 2015, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal, prestó también atención a los delitos de pornografía infantil, tipificando el simple uso o la adquisición de contenidos con esa índole, e incluyó un nuevo apartado para sancionar a quien accediera a contenidos de pornografía infantil a sabiendas a través de las TIC. Igualmente introdujo un apartado para sancionar a aquel que contactase con un menor de dieciséis años y realizase actos con el fin de que este le facilitase material pornográfico o mostrase imágenes de ese carácter. De esta manera, se dio protección a los menores frente a los abusos cometidos en las redes.

Por otro lado, la reforma lleva a cabo la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal. Lo que se hizo fue distinguir entre la revelación de secretos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que menoscaban la privacidad, pero no directamente la intimidad personal. También se modificaron los delitos contra la propiedad intelectual en aras a luchar contra la vulneración de los derechos de autor en la red de Internet[17].

A continuación, mencionaremos y explicaremos brevemente las instituciones públicas y privadas en materia de la ciberseguridad. Además de contar con la normativa que regula los ciberdelitos, tanto en el plano nacional como internacional, España ha dado respuesta en el plano de la ciberseguridad, mediante la creación de varios organismos e

[16] Martínez Sánchez. M.T.: "Incidencia de la última reforma del Código Penal por LO 1/2015, de 30 de marzo, en materia de violencia de género. Especial referencia a la agravante de género y a los nuevos delitos de *stalking* y *sexting*.", El Derecho, Lefebvre, noviembre, 2016, Visto el día 13/9/2020 en web: https://elderecho.com/incidencia-de-la-ultima-reforma-del-codigo-penal-por-lo-12015-de-30-de-marzo-en-materia-de-violencia-de-genero-especial-referencia-a-la-agravante-de-genero-y-a-los-nuevos-delitos-de-stalking-y-sex

[17] Barrio Andrés, M.: "Ciberdelitos: Amenazas criminales del ciberespacio", Editorial Reus, 2017, Madrid, págs. 56-58.

instituciones públicas y privadas, que son claves para la cooperación que se pronuncia en la exposición de motivos del Convenio sobre Ciberdelincuencia.

Siguiendo esta línea, encontramos en el ámbito policial la Unidad de Investigación Tecnológica, que se encuentra dentro de la Comisaría General de Policía Judicial. Su función es la de investigar y perseguir las actividades delictivas en las que tengan incidencia las TIC y aquellos delitos de ámbito nacional y transnacional. Igualmente, actúa como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía (CNP). Bajo la dependencia de esta unidad, se encuentran la Brigada Central de Investigación Tecnológica y la Brigada Central de Seguridad Informática. La primera tiene por objeto la investigación de las actividades que se cometen a través de las TIC, así como la obtención de pruebas y persecución de los delincuentes para ponerlos a disposición judicial. La segunda se centra en investigar las conductas delictivas que repercuten en seguridad y fraudes.

Otro organismo que colabora contra la ciberdelincuencia es la Guardia Civil. Desde 1996 existe en ella el Grupo de Delitos Telemáticos (GDT). Su creación es producto también del afán de investigar los delitos que se cometen a través de los sistemas de información o contra éstos. El GDT cuenta con Equipos de Investigación Tecnológica en todas las provincias.

Asimismo, encontramos más instituciones que apoyan la lucha contra la ciberdelincuencia; por ejemplo, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), creado en 2007, cuyas funciones son impulsar, coordinar y supervisar todas las actividades que dependen de la Secretaría de Estado de Seguridad del Ministerio del Interior. En otras palabras, se encarga de organizar los mecanismos necesarios para garantizar la seguridad de las infraestructuras telemáticas. Otro ejemplo es el Centro Criptológico Nacional, cuya tarea está más enfocada a coordinar la acción de diferentes organismos de la Administración que empleen medios o procedimientos de cifrado, asegurando la fiabilidad de las TIC en ese ámbito. Por último, el más reciente ha sido el Equipo de respuesta a ciberincidentes en infraestructuras críticas y estrategias (CERT), dependiente del Instituto Nacional de Ciberseguridad de España (INCIBE)[18].

[18] Magaz Álvarez, R.: "Criminalidad y Globalización. Análisis y estrategias ante grupos y organizaciones al margen de la ley", Instituto Universitario General Gutiérrez Mellado, Madrid, 2016, págs. 232-235.

Igualmente, es conveniente explicar brevemente la legislación española en materia de Ciberseguridad. En este sentido encontramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, producto de la entrada en vigor del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD). Este reglamento se integró en nuestro ordenamiento jurídico a través de la LOPD. El objetivo principal es proporcionar las directrices que tienen que seguir las empresas respecto al uso de las nuevas tecnologías, garantizando de esta forma que no se vulnerarán los derechos fundamentales de los ciudadanos, entre ellos, los derechos que afectan a la esfera personal. Para ello, se deberán cumplir los principios y técnicas y medidas que contenga el RGPD. También se protege de esta manera a los ciudadanos, otorgándoles un mayor control sobre sus datos personales, materializándose en unos determinados derechos.

Por otra parte, encontramos la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores, aplicable en el supuesto de que el autor sea un menor cuya edad esté comprendida entre los catorce y dieciocho años.

Por último, se hace referencia a la LECrim, como norma reguladora del procedimiento penal que se inicia por la comisión de un ciberdelito.

CAPITULO TERCERO
Clasificación delictual

1. Tipos de Ciberdelitos

1.1 Delitos contra la libertad e indemnidad sexual, la intimidad y el honor

Nos referiremos a los delitos ciberintrusivos, en los que el sujeto activo tiene como fin apoderarse de elementos personales de terceros a través de las TIC[19].

Los delitos de esta índole más típicos son los siguientes:

A) Child grooming o acoso sexual a menores través de la Red

Este tipo de delito consiste en mantener contacto con un menor de edad a través de Internet o cualquier otra TIC, proponiéndole concertar un encuentro con el fin de cometer

[19] Velasco Núñez, E.:" Los delitos informáticos", Sepín Editorial Jurídica, núm. 81, diciembre, 2015, pág. 20.

alguno de los delitos recogidos en los artículos 183 y 189 CP, o con el fin de convencerle a que facilite material pornográfico o le muestre imágenes pornográficas en que se represente o aparezca un menor. En otras palabras, son "aquellas acciones preconcebidas que lleva a cabo un adulto a través de Internet para ganarse la confianza de un menor de edad y obtener su propia satisfacción sexual mediante imágenes eróticas o pornográficas que consigue del menor, pudiendo llegar a concertar un encuentro físico y abusar sexualmente de él"[20].

Nuestro legislador deja regulado este delito en el art. 183 ter CP, atendiendo en su momento al Convenio del Consejo de Europa sobre la Protección de Niños contra la Explotación y el Abuso Sexual, de 25 de octubre del 2007, que en su art. 23 establecía la necesidad de tipificar como delito las proposiciones a niños con contenido sexual a través de las TIC.

La pena será de prisión de uno a tres años o multa de doce a veinticuatro meses, pero se prevén penas agravadas en su mitad superior cuando dicho acercamiento tenga lugar a través de la coacción, intimidación o engaño[21]. Igualmente, cuando el fin sea embaucar al menor para que envíe al autor mensajes, fotografías o cualquier clase de material de contenido sexual en el que aparezca un menor, el reo será sancionado con penas de 6 meses a 2 años de prisión.

Es un delito de mera actividad, pues se entiende consumado cuando se realizan las acciones típicas tendentes al acercamiento[22], y la naturaleza del delito es de peligro, debido a que "no se configura atendiendo la lesión efectiva del bien jurídico protegido sino a un comportamiento peligroso para dicho bien" (STS 692/2017, de 22 de febrero de 2017).

Hay una discusión dogmática respecto a qué bien jurídico se protege; a tenor de ello citamos la STS nº. 97/2015, de la Sala segunda, de lo penal, del Tribunal Supremo, de 24 de febrero de 2015, que indica que el bien jurídico protegido es la indemnidad sexual y la integridad moral del menor: "El bien jurídico tutelado en el precepto es sin duda la indemnidad sexual del menor, indemnidad que hay que entender en su sentido más pleno de contenido pues no solo pretende preservar el derecho a su pleno desarrollo y formación

[20] Panizo Galende. V.: "El ciber-acoso con intención sexual y el *child-grooming*", pág. 23. Visto en web: https://fliphtml5.com/fgec/iizr/basic el 16 de diciembre de 2020.
[21] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, artículo 183.1 ter.
[22] Abadías Selma. A.: "El peligro de la sobreexposición de los menores a internet frente al *child grooming* en tiempos del covid-19", La Ley Penal, Wolters Kluwer, núm.144, mayo-junio de 2020, págs. 4 y ss.

y socialización del menor, así como su libertad sexual futura, sino también su integridad moral, por lo que el favorecimiento o promoción de la prostitución supone de "cosificación" del prostituido".

B) Descubrimiento y revelación de secretos: *Sexting y hacking*

Se trata de delitos de revelación de secretos, a través del apoderamiento y posterior difusión de datos sensibles registrados en ficheros y soportes informáticos[23].

- *Sexting*

Cada vez es más habitual la práctica de *sexting*, sobre todo entre adolescentes o jóvenes de mediana edad. El factor que ha incidido principalmente en esta nueva forma de conducta es la revolución tecnológica, que ha facilitado la realización y difusión de imágenes. No obstante, estos nuevos hábitos pueden llevar aparejadas unas consecuencias lesivas para bienes jurídicos protegidos importantes, tales como el honor, la propia imagen y la intimidad.

Es entendida como la difusión de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual entre personas que voluntariamente consienten en ello. Sin embargo, es una práctica peligrosa en el sentido que existe el riesgo de una pérdida de control de esas imágenes, afectando directamente a la intimidad de la víctima, y, debido a que son transmitidas a través de las TIC, pueden ser difundidas con mayor rapidez y a múltiples personas, lo que trae consigo una mayor intensidad en la lesión del bien jurídico protegido[24].

Dicha conducta está tipificada en el art. 197.7 CP: "[…] el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona". La pena será de prisión de tres meses a un año o multa de seis a doce meses.

Nuestro legislador prevé una agravante, aumentando la pena tipo a su mitad superior, en el caso de que quien difunda las imágenes sea el cónyuge o persona con la que el autor del hecho mantenga una relación afectiva, sin que sea necesario que convivan; o bien, si

[23] Espinosa Sánchez, J.F.: "Ciberdelincuencia. Aproximación criminológica…", op. cit., pág. 156.
[24] Puyol, J.: "¿Qué es y en qué consiste el *sexting*?, agosto 2020. Disponible en: https://confilegal.com/20200817-que-es-y-en-que-consiste-el-sexting/ Visto el 17 de diciembre de 2020.

la víctima es menor de edad o discapacitada; o los hechos se hayan cometido por un fin lucrativo.

- Hacking

La conducta básica se encuentra regulada en el art. 197 bis CP, y castiga al que "por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo".

Por tanto, se castiga el acceso no autorizado, violando los mecanismos de seguridad que hubiera en su caso, a archivos contenidos en un sistema informático ajeno. Es decir, la conducta afecta tanto al equipo informático y, además, puede ser utilizado como herramienta para cometer otros, como al uso de malwares. Igualmente, se castiga a quien produzca y adquiera dicha información no autorizada para su uso, o para importarla o facilitarla a terceros[25].

C) Stalking o acoso informático

Se trata de un delito de coacciones, cuya regulación encontramos en el art. 172 ter CP, que castiga al que "acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana […]". Es un delito incluido en el CP en el año 2015 a través de la LO 1/2015. Para este delito, el CP establece una pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses.

Asimismo, observamos que, para apreciar el delito, debe llevarse alguna conducta de las que establece el precepto, es decir, las conductas punibles por las que se puede incurrir en dicho tipo son: a) vigilancia, persecución o búsqueda de cercanía física; b) establecimiento o intento de contacto con ella a través de medios de comunicación o terceras personas; c) hacer uso indebido de datos, contratando productos o servicios, así como hacer que una tercera persona contacte con la víctima; d) atentar contra su libertad o patrimonio, o contra la libertad o patrimonio de otra persona próxima a la víctima.

Si la víctima fuera vulnerable a causa de su edad, enfermedad o situación, la pena se agravará a una pena de prisión de seis meses a dos años. De igual modo, se agravará

[25] Sánchez Canet, J.: "Cibercriminalidad: especial…", op. cit. pág.23

cuando exista una relación conyugal o de afectividad, tal como determina el art. 172 del CP, pero en ese supuesto no será necesario denunciar, tal como indica el párrafo cuarto del art. 172 ter del CP, que exige para todos los demás supuestos que previamente haya una denuncia de la persona agraviada o de su representante legal, es decir, no es un delito perseguible de oficio, sino a instancia de parte.

El bien jurídico que intenta proteger el legislador con la incorporación del precepto mencionado con anterioridad, tal como expone la STS número 324/2017, de 8 de mayo, de la Sala Segunda, de lo Penal, del Tribunal Supremo, es la libertad. La sala del Alto Tribunal entiende que ésta "queda maltratada por esa obsesiva actividad intrusa que puede llegar a condicionar costumbres o hábitos, como única forma de sacudirse la sensación de atosigamiento". De igual forma, el Alto Tribunal exige implícitamente que la conducta tenga "una cierta prolongación en el tiempo; o, al menos, que quede patente, que sea apreciable, esa voluntad de perseverar en esas acciones intrusivas, que no se perciban como algo puramente episódico o coyuntural, en ese caso no serían idóneas para alterar las costumbres cotidianas de la víctima".

El delito de cyberstalking es aquel que utiliza los medios de comunicación para contactar con la víctima, de forma reiterada, llegando al hostigamiento. En opinión de Alonso de Escamilla, "A consecuencia de la irrupción de las nuevas tecnologías y de su avance y generalización y del enorme crecimiento de Internet durante la última década, se plantea la necesidad de regular los sistemas de transmisión y flujo de toda la información que circula por la Red". Esta apreciación la observamos con la reforma que se produjo en el CP en el 2015, añadiendo un precepto donde quedase regulado el acoso informático o cyberstalking. Y continúa diciendo: "Así el cyberstalking se puede considerar una conducta de acoso u hostigamiento repetitivo que se lleva a cabo en contra de la voluntad de la víctima, utilizando alguna de las herramientas que proporciona Internet, como son e-mail, chat, mensajes de texto, WhatsApp, redes sociales como Facebook o Twitter, páginas webs, o cualquier otro medio de cyberstalking"[26].

1.2 Delitos contra el patrimonio y el orden socioeconómico

Hablamos en concreto de los delitos de defraudaciones, daños, contra la propiedad intelectual e industrial, mercado y consumidores, contemplados en el Título XIII del

[26] Alonso de Escamilla, A.:" El delito de stalking como nueva forma de acoso. Cyberstalking y nuevas realidades", La Ley Penal, núm. 105, noviembre-diciembre, 2013, pág.9.

Libro II CP, bajo el nombre "Delitos contra el patrimonio y contra el orden socioeconómico". Como veremos, todos ellos tienen en común que se cometen mediante las nuevas tecnologías o que afectan a estas, y su fin es la obtención de una recompensa económica, que consiguen sirviéndose de aquellas según el modo de ejecución. Los principales perjudicados, víctimas de este delito, son las pequeñas y medianas empresas, así como las multinacionales, es decir, estamos hablando del sector privado, que es el principal foco de ataques por su poder económico. Es por este motivo que hacemos hincapié en la importancia de contar con ciberseguridad en este sector; gracias a ella se implantan métodos capaces de identificar, bloquear y neutralizar las amenazas que puedan sufrir los equipos y sistemas, y se prevé la seguridad de los mismos, así como la salvaguarda de los datos de los clientes[27].

Uno de los ámbitos del sector privado que más se ha visto afectado en los últimos años es el sector financiero, con motivo de la creación de nuevas modalidades de pago unidas a las tecnologías.

A continuación, analizaremos brevemente aquellos delitos que se encuentran dentro del Título al que nos hemos referido con anterioridad, y que también son denominados como "delitos ciberеconómicos", puesto que el bien jurídico protegido por nuestro ordenamiento es el patrimonio, y este tipo de delitos tienen en común que atentan contra el mismo, pero con un proceso de ejecución diferente, que es lo que caracteriza a cada uno, así como las penas asociadas a esa conducta ilícita.

A) Estafa informática

Se trata de uno de los ciberdelitos más denunciados en nuestra sociedad, y regulado en el art. 248 del CP, donde se considera reos a: a) "Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"; b) "Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo"; y c) "Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero".

[27] Espinosa Sánchez, J.F.: "Ciberdelincuencia. Aproximación criminológica…", op. cit., pág.159.

Estas conductas encajan en el tipo de fraude informático, una modalidad de estafa con disposición propia, que no responde a la forma tradicional de la estafa[28]. Su regulación surge como respuesta al uso de las nuevas tecnologías, creando tipos penales para proteger el patrimonio de los ataques que se cometen a través de aquéllas. A diferencia de las estafas tradicionales, no se basan en la relación interpersonal del autor y víctima, sino del empleo de las TIC para llegar a cometer un daño a la víctima, siendo ésta engañada para conseguir el beneficio patrimonial[29].

Por ende, entendemos por ciberfraudes todas las conductas defraudatorias realizadas mediante los sistemas y/o herramientas informáticas (por ejemplo: introducción de datos falsos en sistemas, manipulación, borrado o supresión de datos, alteración de los programas, etc.)[30].

Observamos también que en el Convenio de Budapest se expone la necesidad de tipificar como delito "toda manipulación indebida realizada en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes".

A modo de conclusión, y en palabras de Galán Muñoz, la estafa informática comporta "abusos que se realizan mediante el uso de nuevas tecnologías y que tratan de obtener un enriquecimiento patrimonial a costa de la consecución de una transferencia de activos que determina la merma patrimonial de un tercero"[31].

Los reos de estafa serán castigados con una pena de prisión de seis meses a tres años, en virtud del art. 249 del CP y se valorará el importe de lo defraudado, el perjuicio económico causado a la víctima y las relaciones entre éste y el defraudador, los medios empleados por el mismo y "otras circunstancias que sirvan para valorar la gravedad de la infracción".

El bien jurídico protegido es el patrimonio de una persona individual. Se trata de un delito que podrá ser cometido por cualquier persona, y tal como menciona el art. 248.2.a), "valiéndose de alguna manipulación informática o artificio semejante".

En cuanto al tipo subjetivo, el injusto típico de esta figura no solo exige que se cometa la conducta de forma dolosa, sino además con ánimo de lucro. Por ende, si un

[28] Sentencia del Tribunal Supremo, núm. 845/2014, Sala de lo Penal, de 2 de diciembre.
[29] Martín, M, A.M.: "Estafas informáticas: tipificación…", op. cit., pág.3.
[30] Ibidem, págs. 4. y ss.
[31] Galán Muñoz, A.: "Los ciberdelitos en el ordenamiento español", Editorial UOC, Barcelona, 2019, pág.139.

sujeto manipula un sistema informático sin la finalidad de enriquecerse o enriquecer a otro, sino para ocasionar un daño a la víctima, no encajaría en este tipo.

Por otra parte, las nuevas modalidades de operaciones bancarias, como la banca online, la utilización de nuevos métodos de pago electrónicos o digitales que han facilitado las transacciones a nivel nacional e internacional, y la dinamización del comercio electrónico, ahora aún más promovido por la situación de pandemia, han favorecido la aparición de nuevas técnicas de comisión de fraude, nuevas modalidades de ataque donde se emplean las propias TIC para acceder a la víctima. Además, como venimos diciendo, la capacidad de conectividad de internet y la eficacia y alcance que tiene, ha facilitado la difusión masiva de engaños y la ejecución de técnicas o maniobras defraudatorias.

Las manifestaciones delictivas de mayor incidencia son: phishing, pharming, ventas fraudulentas a través de páginas webs y carding.

- Phishing y pharming

El objetivo es realizar transferencias económicas no consentidas tras captar las claves bancarias de los perjudicados.

El phishing utiliza el engaño para obtener fraudulentamente de los usuarios información personal, sobre todo las claves de acceso a los servicios financieros. Lo hacen a través del envío de correos electrónicos masivos cuyo contenido es engañoso, o la creación de páginas webs fraudulentas con apariencia de páginas oficiales de entidades bancarias o instituciones de confianza para que la víctima entre en ellas y proporcione sus datos reservados.

El pharming constituye una modalidad de fraude en la que no existe engaño previo para la entrega de información personal o claves bancarias por parte de los titulares de las cuentas, sino que los delincuentes, a través de programas informáticos piratas, realizan una manipulación en el sistema operativo de los ordenadores que van a atacar, consistente en redireccionar de forma malintencionada al usuario a un sitio web falso y fraudulento mediante la explotación del sistema DNS[32].

- Operaciones de ventas fraudulentas en Internet

[32] Magaz Álvarez, R.: "Criminalidad y Globalización. Análisis y estrategias …", op. cit., págs. 45-46.

Consiste en vender con engaño objetos de diferente índole ofertados en portales o páginas webs especializadas. En consecuencia, son incontables las víctimas potenciales. Utilizan principalmente canales o medios de pago donde después es difícil recuperar el dinero, puesto que el autor difumina o elimina el rastro para la no localización.

B) Cracking o daños informáticos

Este ciberdelito se encuentra regulado en el art. 264 del CP. También denominado *cracking*, la diferencia respecto al delito tradicional de daños está en el resultado de este tipo de conducta, pues no solo ocasiona un daño patrimonial, sino que afecta a la integridad y disponibilidad de los sistemas informáticos. Dicho artículo enuncia la conducta básica del delito de daños informáticos: "El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave".

La pena que se impone al reo es de prisión de seis meses a tres años. Los rasgos característicos de este ciberdelito son: haberse realizado sin autorización, es decir, sin consentimiento por parte del propietario o titular del derecho sobre el sistema o parte de este, y además ser grave. Respecto a este punto hay que dejar claro que la gravedad se evaluará en función del daño que ocasione la conducta. Este delito solo se castiga de forma dolosa para dañar, deteriorar, alterar, suprimir o hacer inaccesibles los datos, programas o documentos electrónicos, pero no por parte del propietario o titular del derecho, sino por un tercero ajeno a esos datos o programas, y actuando sin autorización.

Este ciberdelito se agravará, pudiendo imponerse pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en la conducta concurra alguna o algunas de las circunstancias que recoge el art. 264 del CP[33].

Avanzamos por el CP y encontramos la conducta denominada "DoS o Denegación del servicio", regulada en el art. 264 bis del CP, una variante de delito de daños, es decir, un subtipo, estableciendo que: " Será castigado con la pena de prisión de seis meses a tres

[33] Comisión por medio de una organización criminal; daños de especial gravedad o afectando a un número elevado de sistemas informáticos; que el hecho haya perjudicado gravemente el funcionamiento de los servicios públicos esenciales o la provisión de bienes de primera necesidad; los hechos hayan afectado al sistema informático de una estructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la UE o de un estado miembro de la UE; y que el hecho se haya cometido empleando alguno de los medios que cita el art. 264 ter.

años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica".

Por tanto, la conducta típica es obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno o compartido, de forma grave, y sin estar autorizado para ello.

Este ciberdelito también se sanciona con pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado cuando en los hechos concurra alguna de las circunstancias del art. 264.2 del CP.

Por último, encontramos el art. 264 ter, también un subtipo del art. 264, que tipifica el hecho de que un sujeto facilite la comisión de las conductas reguladas en los dos artículos anteriores, de forma que, sin la debida autorización, facilite a terceros: a) un programa informático cuyo fin es cometer alguno de los delitos a que se refieren los artículos 264 y 264 bis; o b) una contraseña de ordenador, código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Si alguna de las conductas ilícitas mencionadas en los tres artículos anteriores ha sido cometida por una persona jurídica, será de aplicación el art. 264 quater, que establece las penas para este tipo de personas.

C) Delitos contra la propiedad intelectual e industrial

La aparición de las TIC y las posibilidades que ofrece la Red han permitido acceder a las obras protegidas por derechos de autor de manera imperceptible, sobre todo a creaciones musicales, audiovisuales, o fotográficas, y en menor medida, a creaciones literarias y científicas. Por este motivo, con la reforma del CP en el año 2015, el Legislador tuvo en cuenta la presencia e importancia de las TIC y cómo estaban contribuyendo al detrimento de la propiedad Intelectual e Industrial, ocasionando perjuicios a los autores.

- Delitos contra la propiedad Intelectual

Para prevenir conductas que vulneraran los derechos de autor a través de las nuevas tecnologías, y aprovecharse de las ventajas que ofrece Internet, nuestro legislador modifica sustancialmente el art. 270.1 CP.

En dicho artículo se dispone que: "Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios". En la anterior redacción, el ánimo de lucro constituía un agravante y con la nueva redacción se encuentra recogido en el tipo básico.

Para comprender mejor a qué se refiere el legislador con beneficio económico directo o indirecto, hay que atender al contenido de la Circular de la Fiscalía General del Estado 8/2015: "En la interpretación del requisito del ánimo de lucro los Sres. Fiscales habrán de tomar en consideración la doctrina sentada al respecto por la Circular 1/2006 a cuyo tenor dicho elemento intencional ha de entenderse como ánimo de lucro comercial, quedando al margen de la persecución penal aquellos comportamientos que pretenden la obtención de algún tipo de ventaja o beneficio distinto del comercial". Y prosigue diciendo que el ánimo de lucro podrá materializarse a través de contraprestaciones económicas (beneficio directo) o mediante ingresos publicitarios o comercialización de datos de usuarios (beneficio indirecto). Por tanto, la nueva redacción amplia el ámbito de actuación del delito[34]. La conducta castigada es la explotación de un producto ajeno sin autorización de quien tenga derechos de autor sobre él.

Por otra parte, el art. 270.2 CP regula la conducta de acceso de contenido ilegítimo en Internet, sancionando a quien "con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente,

[34] Porta Frutos, C.:" El ánimo de lucro en la defensa penal de los derechos de autor", *The Law Clinic*, ECIJA, febrero, 2019. Disponible en web: https://ecija.com/el-animo-de-lucro-en-la-defensa-penal-de-los-derechos-de-autor/ visto el 14 de diciembre de 2020.

aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios".

En estos supuestos, el juez retirará el contenido objeto de la infracción o mandará interrumpir el canal por donde se esté prestando o el bloqueo a su acceso, cuando se cometa reiteración, así como la adopción de cualquier otra medida cautelar para proteger los derechos de propiedad intelectual, en virtud del art. 270.3 CP. Para estos tipos de delitos, el CP establece la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses; sin embargo, si la conducta se realizó de forma ocasional o ambulante, y con un escaso beneficio económico, y siempre que no concurra alguna circunstancia recogida por el art. 271 CP[35], se aplicará una pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

De la misma manera, es destacable lo que establece el art. 270.5 CP, que castiga a quienes importen, almacenen contenido protegido o favorezcan o faciliten las conductas tipificadas en los apartados 1 y 2 del mismo artículo, sin el debido consentimiento y con la finalidad de obtener un lucro directo o indirecto.

Asimismo, este ciberdelito tiene agravantes recogidos en el art. 271 CP; cuando concurra alguna de esas circunstancias, la pena a imponer será de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido.

- Delitos contra la Propiedad Industrial

Este tipo de ciberdelito llama especialmente nuestra atención dada la escasa regulación que hace el legislador al respecto, pues, atendiendo al artículo que lo regula, 274 CP, el tipo básico castiga al que con fines industriales o comerciales, sin consentimiento del titular que ostenta un derecho de propiedad industrial registrado, "fabrique, produzca o importe productos que incorporen un signo distintivo idéntico o confundible con aquel" o bien, "ofrezca, distribuya, o comercialice al por mayor productos que incorporen ese signo distintivo idéntico o confundible […] para los que el derecho de propiedad industrial se encuentre registrado". No se especifica medio concreto

[35] A) Beneficio económico de gran trascendencia; B) Hecho de especial gravedad; C) Sujeto activo perteneciente a una organización criminal; D) Uso de menores para la comisión del delito.

alguno ni en el tipo básico ni en los siguientes artículos; por tanto, entendemos que se incluye la realización a través de cualquier sistema de información[36].

D) Delitos relativos al mercado y a los consumidores

Se trata de delitos que se cometen cuando se desvelan secretos o se viola la intimidad de la persona jurídica sin su debido consentimiento. El tipo básico lo encontramos en el art. 278 CP, que castiga al que, "para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197[…]". Por "cualquier medio" entendemos que pueden incluirse aquellos informáticos, por ello lo encajamos como un ciberdelito, penado con prisión de dos a cuatro años y multa de doce a veinticuatro meses, como continúa el artículo diciendo. La conducta castigada es apoderarse de una determinada información empresarial sin la autorización de quien corresponda. Aún peor será cuando el ciberdelincuente difunda, revele o ceda a terceros los secretos descubiertos, llevando aparejada una pena de prisión de tres a cinco años y multa de doce a veinticuatro meses[37]. Es decir, la difusión o cesión a terceros agrava la pena base. No debemos confundir la información que se obtiene y revela con el *know how* de una empresa, que contiene la realización de las tareas y se revela a causa de una relación mercantil. Ni tampoco con los denominados atributos de la libre competencia, los cuales se obtienen por mantenerse en el mercado[38].

Otro delito cibereconómico es el que encontramos dentro del Título XVIII del Libro II, "de las falsedades", concretamente hablamos del artículo 399 bis, que regula la falsificación de tarjetas de crédito y débito y cheques de viaje.

La conducta punible que recoge dicho artículo es la copia, reproducción u otro modo de falsificación de aquellos medios de pago o cheques de viaje. No es estafa informática, porque la principal diferencia entre una y otra es que, en el delito de estafa, media el engaño en la conducta, no hay falsedad en las tarjetas que se utilizan, sino la ausencia del consentimiento para usarlas o un vicio en el mismo, sin embargo, en esta figura es el objeto material del delito el que es falso. Tal delito comporta dos conductas:

[36] Barrio Andrés, M.: "Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010", La ley penal, Wolters Kluwer, núm. 86, octubre 2011, pág.16.
[37] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 278.2.
[38] Velasco Núñez, E.: "Los delitos informáticos", op.cit., pág.22.

por un lado, la fabricación de la tarjeta o cheque de viaje mediante programas informáticos, o incorporando conductas ficticias y, por otro lado, sus componentes físicos permiten la posterior suplantación de identidad o tráfico en el mercado[39]. El reo que cometiera este ciberdelito será castigado con la pena de prisión de cuatro a ocho años.

Cabe destacar la práctica de clonado de tarjetas, conocido como *skimming*. Esta práctica supone copiar la banda magnética mediante el robo de información de la tarjeta en el momento en que la víctima realiza una transacción. Con esta conducta, el ciberdelincuente puede utilizar la tarjeta y los datos asociados a la misma para compras online o suplantación de identidad en comercios físicos, entre otros, como hemos mencionado.

Además, nuestro legislador aumenta la pena cuando los efectos de la conducta repercutan a una pluralidad de personas o se cometa en el seno de una organización criminal.

1.3 Delitos contra el orden público

Dentro del Título XXII del Libro II CP, encontramos en su capítulo VII los delitos de terrorismo, concretamente aquellos de ciberterrorismo. En 2008, la OTAN describió el ciberterrorismo como "un ciberataque usando o explotando redes informáticas o de comunicación para causar una destrucción o disrupción suficiente para generar miedo o intimidar a una sociedad dirigiéndola hacita una meta ideológica"[40]. En opinión de Pérez Gómez, hay dos tipos de acciones ciberterroristas: el ciberterrorismo puro, aquel que busca causar un daño exclusivamente a través de las TIC, y, por otro lado, las acciones de apoyo al terrorismo tradicional mediante actos de ciberterrorismo tales como la financiación, reclutamiento, adiestramiento, etc.[41].

A través de este tipo de delitos, el sujeto activo pretende crear terror y atemorizar a una masa de la población por medio del uso de las TIC, debido a que aportan una gran cantidad de información necesaria para planificar y cometer un ataque terrorista y permiten la comunicación y creación de vínculos entre los terroristas, así como para

[39] Sánchez Canet, F.J.:" Cibercriminalidad: especial referencia al delito de usurpación y suplantación de identidad", Trabajo de Fin de Máster, Universidad Internacional de la Rioja, Valencia, 2016, pág. 21.
[40] González-García. A., y Girao González, F.J.: "Capacidades prospectivas y de defensa en la lucha contra el ciberterrorismo: análisis del caso español", Revista de Relaciones Internacionales, Instituto de Relaciones Internacionales, UDIMA, núm.68, junio,2020, Madrid, pág.242. Disponible en web: https://dialnet.unirioja.es/servlet/articulo?codigo=7529103 visto el 4 de marzo de 2021.
[41] Pérez Gómez, A.: "Ciberterrorismo, ¿una nueva amenaza?", Instituto Español de Estudios Estratégicos, núm.19, septiembre, Madrid, 2020, pág.243.

realizar campañas de propaganda de adoctrinamiento[42]. Estos ataques aumentan el riesgo de que las infraestructuras críticas se vean afectadas, produciéndose un colapso de varias dimensiones en la sociedad o a nivel transnacional[43].

Por tanto, en palabras de Pons Gamón, es la forma más destructiva de ciberdelincuencia, ya que usa las TIC para lograr sus objetivos terroristas, intimidando, atemorizando y causando daños a sus víctimas. Hoy por hoy, los ataques terroristas, tanto en su preparación como en su ejecución, se apoyan en el ciberespacio o utilizan las TIC en la realización de la acción[44].

A) Adoctrinamiento y adiestramiento terrorista

Nuestro ordenamiento castiga con pena de prisión de dos a cinco años a los sujetos que reciban adoctrinamiento o adiestramiento con la finalidad de capacitarse para cometer un delito terrorista. El art. 575 del CP entiende que "comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos […] para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines".

B) Enaltecimiento del terrorismo

La conducta básica consiste en la "participación en la ejecución o realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de ataques terroristas o de sus familiares". La pena de esta conducta (prisión de uno a tres años y multa de doce a dieciocho meses) puede ser agravada en su mitad superior, si los hechos a los que se refiere el art. 578 se hubieran llevado a cabo mediante la difusión a través de las TIC.

C) Difusión e incitación al terrorismo

Se castiga en el art. 579 del CP la difusión pública de mensajes o consignas que persigan incitar a otros para la comisión de un delito terrorista. En caso de que la difusión

[42] Velasco Núñez, E.: "Los delitos informáticos", op. cit., pág.23.
[43] Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad, Estrategia Nacional de Ciberseguridad, Gobierno de España, 2019, pág.26.
[44] Pons Gamón, V.: "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad", URVIO, Revista Latinoamericana de Estudios de Seguridad, Ecuador, núm. 20, julio, 2017, pág.85.

se hubiera hecho a través de las TIC, el órgano jurisdiccional competente ordenará la retirada de los contenidos. De forma subsidiaria, el órgano jurisdiccional podrá solicitar a los prestadores de servicios de alojamiento, motores de búsqueda y proveedores de servicios de comunicaciones electrónicas la retirada del contenido ilícito, la inaccesibilidad al mismo o la eliminación de los enlaces que dirigen a estos.

CAPITULO CUARTO

EL AGENTE ENCUBIERTO INFORMÁTICO COMO INSTRUMENTO DE INVESTIGACIÓN

1. Concepto y características

Debido a las nuevas modalidades de delincuencia, las técnicas tradicionales de investigación han quedado obsoletas, siendo necesario dotarse de herramientas que aborden los delitos tecnológicos y los delitos tradicionales que puedan verificarse con nuevas tecnologías, como, por ejemplo, conocer la zona y saber desde qué antena un usuario recibe comunicaciones electrónicas sin estar conectado y de esta forma situarlo[45].

Gracias a la reforma de la LECrim de 2015, llevada a cabo por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, se regulan aquellos supuestos en los que un delito se comete a través de las TIC o es objeto de las mismas, es decir, supuestos ocasionados por la evolución de la comisión de actos ilícitos, que en el desarrollo del CP de 1995 no se contemplaron, siendo una de las principales novedades de la reforma la creación de la figura del agente encubierto informático.

El primer punto que abordaremos en este capítulo será el concepto de agente encubierto. Es preciso matizar que, antes de la reforma de la LECrim en 2015, la Ley solo contemplaba la figura del agente encubierto físico, que se introdujo por primera vez con la LO 5/1999, de 13 de enero, de modificación de la LECrim en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas

[45] Vallés Causada, L.: Tecnología aplicada por la Policía a la investigación criminal, "Congreso internacional: la nueva reforma procesal penal: Derechos fundamentales e Innovaciones Tecnológicas", Organizado por el Ministerio de Ciencia y Tecnología y Vicente Gimeno Sendra, coord. del Máster Universitario de Derechos Fundamentales en la UNED, Facultad de Derecho de la UNED, celebrado el 17 de octubre de 2017, visitado el 9 de octubre de 2020 en la web: https://canal.uned.es/video/5a6f55edb1111f655c8b458e

y otras actividades ilícitas graves. La figura del agente encubierto viene regulada en el art. 282 bis LECrim. Para entender mejor su concepto acudiremos a la Sentencia del TS 104/2011, de 1 de marzo, que lo define como "agente de policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o éstos sean manifiestamente insuficientes, para su descubrimiento, y permite recabar información sobre su estructura y modus operando, así como obtener pruebas sobre la ejecución de hechos delictivos". Por tanto, su creación reside en la necesidad de investigar delitos que, debido a los sujetos que lo cometen o por el modo de operar, son difíciles de descubrir.

Una vez conocido el concepto, pasamos a explicar qué figura es el agente encubierto informático, también conocido como *online* o virtual. El agente encubierto informático es una variante del agente encubierto tradicional motivada por la evolución de los delitos debido al desarrollo de las TIC y el aumento de la delincuencia en este ámbito. Como mencionábamos antes, en un escenario de cibercrimen, nuestro Estado de Derecho necesita mecanismos para luchar contra él de manera efectiva. Este es el motivo por el cual el Estado ha incluido en el ordenamiento procesal medios de investigación idóneos, que, respetando los principios constitucionales, penales, y las garantías procesales, permitan llevar a cabo una función investigadora que logre obtener como resultado pruebas de actividades ilícitas que posteriormente puedan sustentar el ejercicio de la acción penal contra los ciberdelincuentes.

En otras palabras, la actuación del agente encubierto físico se queda corta de cara a los escenarios que se presentan cada día en la vía penal, dada la presencia de los ciberdelitos a causa de un aumento en el uso de las TIC. En principio, el agente encubierto físico se crea para investigar aquellos delitos que se producen en el mundo físico; no obstante, el desarrollo de las TIC y el aumento de su uso conlleva cambios en los modos de operar y cometer delitos, lo que conlleva a prever una regulación y establecer sanciones al respecto. Con la reforma de la LECrim, a través de la LO 13/2015, de 5 de octubre, de modificación de esta Ley para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, se incluyen los apartados 6 y 7

del art. 282 bis LECrim, donde queda regulada la figura del agente encubierto informático[46].

El agente encubierto informático ha sido definido por el Tribunal Supremo en la sentencia 140/2019, de 13 de marzo (con cita de otra sentencia 1140/2010, de 29 de diciembre), como "funcionario de la policía judicial que actúa en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito".

Esto se traduce en una modalidad del agente encubierto físico adaptado a las necesidades de lucha contra el cibercrimen y con particularidades dadas por su naturaleza tecnológica, por actuar en el ámbito de las nuevas tecnologías.

Según J. De La Mata, el agente encubierto informático se caracteriza por las siguientes notas[47]:

a) Es una medida de investigación relevante para la determinación del objeto del proceso penal. Por un lado, consigue corroborar la existencia del delito y, gracias a la interacción del agente con los sujetos, se extiende el elemento subjetivo del proceso penal a otros sujetos que al principio no eran sospechosos. Es por tanto un elemento imprescindible en los delitos cometidos por medios tecnológicos en los que interviene una colectividad de sujetos o una organización criminal.
b) Afecta menos que otras diligencias de investigación informáticas a los derechos fundamentales de los investigados. Es menos intrusiva que el resto de las diligencias y, en consecuencia, de conformidad con los principios rectores de las diligencias de investigación tecnológicas reguladas en el art. 588 bis LECrim, deberá adoptarse con preferencia a otras, tales como el rastreo de equipos de forma remota o la captación y grabación de comunicaciones orales mediante el uso de dispositivos electrónicos, pues estas son más gravosas, llegando a afectar al derecho de la intimidad, o al secreto de las comunicaciones de los sujetos investigados.

[46] González García, S.: "El agente encubierto informático a examen: un análisis de su regulación y de la validez de su actividad investigadora y probatoria en el proceso penal", La Ley Penal, núm. 139, julio 2019, Wolters Kluwer, Madrid.
[47] De la Mata, J.: "El agente encubierto online", Congreso Internacional "La Nueva Reforma Procesal Penal: Derechos Fundamentales e Innovaciones Tecnológicas", visitado el 1/10/20 en la web: https://canal.uned.es/video/5a6f55f0b1111f655c8b45a8

c) Para iniciar su actividad es preceptiva la resolución del juez de instrucción, que es el órgano autorizante exclusivo para ello, a diferencia del agente encubierto convencional o físico, que puede ser autorizado por el juez o el Ministerio Fiscal.
d) El agente deberá ser funcionario de la Policía Judicial. Pertenecen a la Policía Judicial los miembros de cuerpos policiales conforme a la Ley Orgánica 2/86, de 13 de marzo, sobre Fuerzas y Cuerpos de Seguridad (LOFCS). Estos ejercen sus funciones en todo el territorio nacional y están integrados por el Cuerpo Nacional de Policía y la Guardia Civil. En virtud del art. 29 LOFCS: "1. Las funciones de Policía Judicial que se mencionan en el artículo 126 de la Constitución serán ejercidas por las Fuerzas y Cuerpos de Seguridad del Estado, a través de las Unidades que se regulan en el presente capítulo. 2. Para el cumplimiento de dicha función tendrán carácter colaborador de las Fuerzas y Cuerpos de Seguridad del Estado el personal de Policía de las Comunidades Autónomas y de las Corporaciones Locales". Igualmente se reconoce la condición de Policía Judicial al Servicio de Vigilancia Aduanera respecto de la investigación de delitos de contrabando y sus conexos, de conformidad con la Disposición Adicional 1ª de la LO 12/95[48], en el Decreto 319/82[49] y en los Acuerdos de Schengen[50]. Respecto a las Policías autónomas de País Vasco y Cataluña, habrá que atender a lo dispuesto en la LOFCS y en los Estatutos autonómicos.

2. Regulación del agente encubierto informático

Tal como hemos expuesto con anterioridad, el agente encubierto se introdujo en la LECrim por primera vez en 1999; en su art. 282 bis se preveía la posibilidad de autorizar a funcionarios de la Policía Judicial para que pudieran actuar bajo una identidad supuesta, con la autorización previa del Juez o Ministerio Fiscal solo para delitos cometidos en el seno de una organización criminal. No obstante, antes de ser introducida ya venía usándose sin regulación, pero su empleo fue avalado por la jurisprudencia de la Sala Segunda del TS. Con la reforma de 2015, se incorpora el agente encubierto informático en el apartado 6 del precepto, en el que se recoge la posibilidad de que un juez pueda autorizar a un funcionario de la Policía Judicial a actuar bajo una identidad

[48] Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.
[49] Real Decreto 319/1982, de 12 de febrero, sobre el servicio de vigilancia aduanera: denominación y reestructuración.
[50] Instrumento de ratificación del Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985.

supuesta en comunicaciones realizadas en canales cerrados de comunicación con el objeto de esclarecer alguno de los delitos a los que se refiere el apartado 4 del art. 282 bis o cualquier otro de los previstos en el art. 588 ter a) LECrim. El legislador crea esta figura para investigar los delitos que se realizan en canales cerrados de comunicación.

Por un lado, el agente encubierto físico se prevé para las "investigaciones que afecten a actividades propias de la delincuencia organizada". La LECrim entiende por delincuencia organizada "la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas, previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos, previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución, previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico, previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial, previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores, previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros, previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada, previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo, previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública, previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos, previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo, previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico, previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando".

Además, forma parte del ámbito objetivo el art. 588 ter a) LECrim, como hemos mencionado, dado que el agente también puede actuar en relación con los delitos regulados en el art. 579.1 LECrim o a través de medios informáticos o cualquier otra TIC o servicios de comunicación. El art. 579.1 LECrim se refiere a los siguientes delitos:

- Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

- Delitos cometidos en el seno de un grupo u organización criminal.

- Delitos de terrorismo.

De su regulación podemos apreciar varias diferencias:

i) De la lectura del apartado 1 y 4 del art. 282 bis se desprende la principal diferencia: ámbito objetivo. El agente encubierto físico es un medio de investigación para los delitos cometidos en el seno de una organización criminal. Sin embargo, en el apartado 6 se autoriza que exista el agente encubierto informático sin necesidad de que el delito se haya cometido en el seno de una organización criminal o terrorista y se extiende el número de delitos en los que puede intervenir. El agente encubierto informático no solo interviene en los supuestos de criminalidad organizada, sino que también en los delitos de terrorismo y en todos aquellos delitos dolosos cuya pena tenga como límite máximo tres años de privación de libertad o bien se trate de delitos cometidos a través de las tecnologías.

ii) Otra de sus diferencias la encontramos en que el agente encubierto solamente puede adquirir o transportar los instrumentos del delito, mientras que el agente informático no se encuentra limitado, pudiendo intercambiar o enviar esos archivos ilícitos por canales cerrados.

iii) Es por ello, con la finalidad de prevenir una posible provocación del delito, por lo que el legislador prevé que la autorización solamente la pueda proporcionar un órgano jurisdiccional, a diferencia del agente encubierto.

iv) El agente encubierto informático, a diferencia del agente encubierto tradicional, no interactúa con los sujetos investigados, ya que su ámbito de acción se produce en canales cerrados cuya identidad permanece en el anonimato.

Desde un plano internacional, el agente encubierto también se encuentra contemplado, debido al incipiente aumento de la actividad delictiva internacional; por ello, cabe señalar que el Convenio de Naciones Unidas contra el Tráfico ilícito de estupefacientes y sustancias psicotrópicas, celebrado el 19 de diciembre de 1988, insta a los participantes a elaborar un protocolo de medidas conjuntas con la finalidad de erradicar dicho problema. Este hecho es la base sobre la que el legislador español se apoya para dar cobertura legal en España a la figura del agente encubierto.

Esta cobertura jurídica también la encontramos en el art. 20 de la Convención de Naciones Unidas contra la Delincuencia Organizada Trasnacional, donde se establece que cada Estado, dentro los principios fundamentales de su ordenamiento jurídico, podrá utilizar técnicas especiales de investigación, como la vigilancia electrónica o las operaciones encubiertas, con el objetivo de combatir de forma eficaz la delincuencia organizada.

Finalmente, en la Convención de Naciones Unidas contra la corrupción, de 31 de octubre de 2003, también encontramos la figura del agente encubierto como respuesta a este tipo de delitos, recogida en su art. 50.1, donde se prevén una vez más las "técnicas especiales de investigación […] y las operaciones encubiertas"[51].

3. Provocación delictiva como límite

[51] Alcolado Chico, M.T.: "La evolución hacia la moderna funcionalidad del agente encubierto: incidencia de las nuevas reglas de la Ley de Enjuiciamiento Criminal", Revista Jurídica de Asturias, núm. 39, noviembre 2016, págs. 20-21.

Una vez que hemos visto la definición del agente encubierto y su respaldo jurídico, vamos a centrarnos en explicar su marco de actuación, y los límites que no puede sobrepasar para que su actuación no desencadene un delito provocado, ya que la línea entre ganarse la confianza de los sujetos investigados e instigarles a delinquir es muy fina.

El agente encubierto informático adquiere o transporta objetos ilícitos, una conducta colaborativa, pero además puede remitir archivos ilícitos, lo que supone una conducta más activa, que puede confundirse con la provocación.

Un delito provocado es aquel en el que una persona induce a través de engaños a otra a cometer un delito que en principio ésta no tenía intención de cometer. En palabras de los magistrados de la Sala de lo Penal del TS en la Sentencia de 18 de abril de 1972, es "aquél que surge por obra y a estímulos de provocación" por parte de un agente provocador que "lo realizará a través de inducción engañosa con el objeto de conocer la propensión al delito de una persona sospechosa y con la finalidad de constituir pruebas indubitables de un hecho criminal, convenciendo al presunto delincuente para que cometa el delito".

Para discernir esta cuestión, el TS, ante la falta de regulación de la LECrim, se ha pronunciado por medio de jurisprudencia. La Sentencia n.º 591/2018, de 26 de noviembre, recoge la doctrina sobre cuándo no estamos ante un delito provocado y señala:

1. Existencia de ánimo delictivo propio en los autores. En los delitos provocados, como hemos indicado, es el provocador quien tiene una intención, que es la de que el provocado cometa un delito, y actúa en base a ella. Por tanto, el provocado no tiene un ánimo delictivo propio, sino que es inducido a ejecutarlo.
2. La actividad policial es meramente investigadora. No hay delito provocado cuando la actuación del agente se dirige a investigar y recabar pruebas y trabaja condicionada a las conversaciones con los implicados, que son los que tienen el animus delictivo.
3. La conducta del agente es consecuencial a la conducta de los investigados. Son los investigados quienes inician la actividad ilícita, no el agente encubierto; éste actuará de forma que reciba información y facilite la detención, pero no provocará la comisión del delito.
4. No debe confundirse la investigación del agente encubierto con tomar la iniciativa el autor de una intención delictiva preexistente. En el delito provocado no existe una conducta previa, puesto que es el agente provocador quien induce a la

comisión del hecho. Sin embargo, cuando actúa el agente encubierto, lo hace de manera que investiga un delito que se está cometiendo, que ya prexistía antes de su entrada.

5. Es delito provocado incitar a cometerlo con actos manifiestos y claros. No será delito provocado cuando la conducta del agente venga determinada por la inicial de los investigados. En un delito provocado la conducta inicial viene dada por el agente provocador, no por los implicados.
6. La labor del agente infiltrado no pretende la comisión del delito. El agente encubierto se limita a investigar y recoger pruebas de delitos ya cometidos o que se están cometiendo o a colaborar con el investigado que previamente habrá buscado esa colaboración con terceros y el agente encubierto aprovecha la oportunidad de ofrecerse para ello adoptando una apariencia de civil o simulando ser delincuente.
7. El dolo en el autor o autores existe antes de la designación del agente encubierto. Los autores actúan de forma libre y voluntaria antes de la intervención del agente encubierto, aquél no crea el dolo en los autores debido a que éstos ya están obrando dolosamente; no es como con el agente provocador, en este supuesto los autores actúan con dolo después de la intervención del agente.
8. Los autores actúan libremente. La actuación policial será licita siempre que permita la evolución libre de la voluntad del sujeto y no suponga una inducción a cometer el delito.
9. La prueba en el delito. En los delitos provocados, la intención del agente provocador es obtener la prueba, una prueba provocada por él mismo al incitar al delincuente a perpetrar una acción, que previamente no tenía propósito de realizar, de forma que, si no hubiera existido aquélla, el delito no se habría producido, puesto que el sujeto inició la actividad por inducción y no por su propia y libre decisión.

De las diferencias que destaca la doctrina, apreciamos que:

i) El agente encubierto sí se infiltra en una organización criminal, no solo se limita a contactar con ella o el delincuente como lo hace el agente provocador.

ii) El agente encubierto puede utilizar una identidad ficticia o simulada, a diferencia del agente provocador, que se limita a ocultar su condición de autoridad pública.

iii) La finalidad del agente encubierto es infiltrarse para indagar y recabar pruebas. Sin embargo, la finalidad del agente provocador es detener al delincuente *in fraganti,* impidiendo el agotamiento del delito.

4. Actuación del agente encubierto informático en la ciberdelincuencia

Es preciso dedicar una breve explicación a este aspecto de gran relevancia, puesto que es necesario saber hasta cuándo y hasta dónde puede actuar un funcionario de la policía judicial sin autorización judicial y cuándo dicha actuación conlleva la vulneración de los derechos fundamentales (secreto de las comunicaciones, derecho a la intimidad, etc.) y, por ende, la nulidad de pruebas obtenidas[52].

El agente de la policía judicial necesitará o no de autorización judicial dependiendo del nivel de infiltración en el que actúe:

a. Ciber-patrullaje

Se trata del primer nivel de infiltración, a través del cual el agente encubierto informático se encarga de rastrear la información de diversos espacios de libre acceso, como redes sociales o foros abiertos de Internet. La función de rastreo es la vigilancia, prevención y evitación de los delitos que tienen lugar en espacios abiertos, es decir, en canales de comunicación abiertos. En otras palabras, se trata de patrullar en Internet como lo haría un policía por las calles en el mundo físico. Los miembros de las Fuerzas y Cuerpos de Seguridad son los encargados de realizar esta técnica en virtud de la prevención del delito[53]. De la lectura de la exposición de motivos de la LO 13/2015 se desprende la no obligatoriedad de solicitar autorización judicial cuando el agente encubierto informático actúe en canales abiertos.

b. Contacto con usuarios

Se trata del segundo nivel de infiltración, a través del cual los agentes de policía mantienen contacto previo con los investigados ocultando su condición en prevención del delito. Normalmente, con la técnica de ciberpatrullaje se consigue obtener algún contacto en un foro abierto y es frecuente que con posterioridad se produzca una invitación a entrar

[52] Artículo 11 LOPJ: *"No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".*

[53] Zaragoza Tejada, J.I.: "El Agente Encubierto Online". En: Bermúdez González, J.A., García Marcos, J., Perals Calleja, J., Tejada de la Fuente, E., Velasco Núñez, E., Zaragoza Aguado, J.A., Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015, Thomson Routers, Navarra, 2017, pág. 335.

en un foro cerrado. Es en ese momento cuando el agente de policía solicita autorización judicial, fundamentado su petición en la existencia de elementos indiciarios de un delito.

c. Infiltración profunda

Es el tercer nivel de infiltración, y requiere en todo caso autorización judicial. Su explicación reside en que esta técnica conlleva de manera inherente la injerencia en el ámbito de los derechos fundamentales. En este sentido, la STC 204/2016, de 10 de marzo, expone que "La razón de ser de la necesidad de esta autorización con carácter generalizado es la consideración de estos instrumentos […] afectan de modo muy variado a la intimidad del investigado […] resulta muy difícil asegurar que una vez permitido el acceso directo de los agente policiales a estos instrumentos para investigar datos […] pueda acceder o consultar también otros datos -protegidos por varios derechos fundamentales, es decir, intimidad (art. 18.1 CE), secreto de las comunicaciones (art. 18.3 CE), protección de datos (art. 18.4 CE)-. Es por ello por lo que el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual".

La autorización judicial es la garantía de legitimidad constitucional, que debe fundamentarse en los siguientes criterios[54]:

i) Idoneidad: Que la actuación del agente encubierto sirva objetivamente para obtener datos útiles para la investigación criminal.
ii) Necesidad: Que existan indicios suficientes que permitan afirmar que el sujeto está cometiendo un delito que encaja en el ámbito objetivo de la actuación del agente.
iii) Proporcionalidad: Que la actuación resulte más ventajosa que otras técnicas, aunque sea en menoscabo de otros valores en conflicto.

El efecto de obtener autorización judicial es la exención de responsabilidad criminal prevista para los agentes encubiertos (art. 282 bis 5 LECrim). Para el agente encubierto informático, es necesaria la resolución judicial para que comience a actuar, pero se exime su responsabilidad criminal cuando su actuación sea consecuencia necesaria del desarrollo de la investigación y sea proporcional a la finalidad de la misma.

[54] Solano de Castro. S: "El Agente Encubierto Informático", Trabajo Fin de Máster, Universidad Complutense, 2020, Madrid, págs. 17-19.

En conclusión, el agente encubierto informático necesitará autorización judicial para actuar en canales cerrados de comunicación y otra autorización para intercambiar o enviar archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos en virtud de su tarea investigadora; dicha autorización es de carácter especial y se hará en la misma resolución con motivación por separado o en otra resolución distinta. Además, el agente encubierto informático podrá navegar sin autorización judicial en foros y páginas webs mientras sean canales abiertos en aras de cumplir su labor preventiva e investigadora del delito. El hecho de no ser necesaria una autorización judicial para navegar bajo identidad supuesta por canales o foros abiertos de Internet deviene de que, habitualmente, los usuarios utilizan un pseudónimo para interactuar y la confianza del resto de usuarios no se ve vería defraudada si un policía judicial ocultase su verdadera identidad[55].

5. Responsabilidad del agente encubierto informático

Cabe preguntarnos si el agente encubierto informático tiene algún tipo de responsabilidad penal por cometer acciones delictivas por el cumplimiento de su función investigadora. Estas acciones pueden ser: escuchas ilegales, falsedad documental, recepción y envío de imágenes de pornografía infantil, etc.

La respuesta nos la da la LECrim en su art. 282 bis, apartado cinco, según el cual "El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito".

Al tratarse el agente encubierto informático de una adaptación a la nueva realidad virtual, y ser una modalidad del agente encubierto, le es de aplicación en los mismos términos la exención de responsabilidad criminal recogida en el artículo señalado en el párrafo anterior.

[55] Agente encubierto online en los registros remotos de equipos informáticos en el proceso penal, Ed. Iberley. Visto en https://www.iberley.es/temas/agente-encubierto-on-line-registros-remotos-equipos-informaticos-proceso-penal-63160 el 17 de octubre de 2020.

Para que el agente encubierto informático se beneficie de la exención de responsabilidad criminal por los delitos que comete a título de autor o partícipe tiene que cumplir los siguientes requisitos[56]:

1. Su actuación debe ser avalada por una resolución judicial.

El agente encubierto informático tiene que haber actuado autorizado por una resolución judicial que le autorice a ello. Igualmente, la actuación de enviar e intercambiar por él mismo archivos de contenido ilícito y analizar los resultados de los algoritmos que aplica para identificar los archivos ilícitos tendrá también que autorizarse por medio de otra resolución que así lo especifique.

La exigencia de una resolución judicial se fundamenta en dos motivos: primero, porque así lo establece la LECrim, en el artículo que recoge todo lo relativo a la actuación del agente encubierto, y segundo, porque es un requisito de procedibilidad, es decir, para que se pueda proceder penalmente contra el agente encubierto informático es necesario previo informe del juez que hubiera autorizado su actuación. Este requisito de procedibilidad obliga a que el agente encubierto informático solicite su intervención[57].

En consecuencia, esta causa especifica de exención de la responsabilidad criminal será de aplicación para el agente que cuente con la autorización debida para actuar como agente encubierto informático. En el supuesto que no tuviera dicha autorización, su responsabilidad criminal se estudiará según las reglas generales del CP.

2. Necesidad

Su actuación tiene que ser consecuencia necesaria del fin que persigue la investigación. Además, la ley no dice nada respecto de la subsidiariedad, pero se entiende implícita en el requisito de la necesidad, debido a que la medida no será necesaria si caben otras medidas menos gravosas para los derechos fundamentales que puedan lograr el mismo fin que se persigue.

3. Proporcionalidad

La comisión de actos ilícitos tiene que ser proporcional al fin de la investigación. Habrá que ponderar el valor que tienen los actos ilícitos y el de la finalidad que persiguen. Como regla general, la finalidad es averiguar quiénes son los autores, cuál es el modus

[56] Delgado Martín, J.: "Medios encubiertos de investigación de la criminalidad organizada", Actualización de la 2ª parte de "La criminalidad organizada", 2017, págs.76-78, disponible en: https://n9.cl/95bbn. Visto el 1 de noviembre de 2020.
[57] Ibidem, págs.74-75.

operandi, y el recorrido del archivo ilícito. Para ello hay que analizar el delito que debe cometer el agente encubierto informático para alcanzar esos fines dichos anteriormente, y también analizar los bienes jurídicos que con su actuación pudieran resultar afectados. Por último, pero no menos importante, hay que analizar la gravedad del delito que se investiga, no solo atendiendo a la pena que se le pudiera imponer, sino también a su transcendencia social o repercusión sobre los bienes que protege nuestro ordenamiento.

En conclusión, para que el agente encubierto informático intercambie o envíe archivos ilícitos y no tenga responsabilidad criminal por ese hecho, necesitará previamente una autorización judicial donde se especifique que el envío o intercambio se hace en virtud de una función investigadora. La autorización se hará ponderando la idoneidad, necesidad y proporcionalidad de su actuación, determinando el archivo, el control de su recorrido y evitando cualquier riesgo de provocación delictiva.

CAPITULO QUINTO

LA PRUEBA DE LOS CIBERDELITOS

1. Requisitos de admisibilidad de la prueba

Es común que los ciberdelitos no lleguen a las instancias judiciales debido a su carácter transnacional y de anonimato, lo que dificulta su persecución, investigación y enjuiciamiento. En este capítulo estudiaremos los requisitos que debe cumplir una prueba para que sea admitida en juicio, los medios de los que disponemos para certificarla y presentarla y cómo es el desarrollo de una prueba pericial informática.

La investigación y prueba de los ciberdelitos son cuestiones complejas, dado que, para averiguar el hecho ilícito y la autoría de éste, hay que tener en cuenta que son cometidos en un espacio virtual caracterizado por la transaccionalidad y anonimato, lo que dificulta en muchas ocasiones conocer el hecho y a sus responsables, además de los equipos informáticos y telemáticos a través de los que se comete el delito.

En esta línea, Mestre Delgado explica que la dificultad de averiguación del autor así como la prueba de los hechos reside en tres motivos complementarios: i) la propia naturaleza de la mecánica comisiva, que facilita la ocultación de autoría gracias a la ocultación de la identidad, sirviéndose de identidades irreales, y a la utilización de técnicas de bloqueo de la trazabilidad de la orden o mensaje con el que se comete el delito;

ii) la inexistencia de previsiones legales concretas que habiliten la intervención de la policía en los ámbitos privados, que usualmente son donde se cometen los delitos; iii) la inexistencia de reglas específicas dentro del ámbito de intervención material de las TIC, es decir, no se concreta el modo de actuación para obtención, custodia y reproducción de los datos contenidos en dichos dispositivos[58].

Cuando nos referimos a prueba informática, el término "informática" abarca la electrónica. En la práctica, la prueba informática es entendida como "toda información generada, almacenada o transmitida mediante el uso de dispositivos informáticos aptos para acreditar el hecho objeto de enjuiciamiento". Delgado Martín define ésta como "toda información de valor probatorio contenida en un medio informático o transmitida por dicho medio". Los medios que señala pueden ser entre otros, un USB, un móvil, un ordenador, un dron, etc.[59]

Mestre Delgado determina que la prueba de los ciberdelitos se articula a través de tres medios diferenciados, es decir, puede presentarse en el proceso de tres formas: como prueba documental, testifical o pericial. En la primera, la documental, se plasman los datos que contiene el dispositivo electrónico o informático en un soporte físico y que permita su lectura (documento impreso u otro sistema de almacenamiento de datos que pueda reproducirse, por ejemplo, un CD). En la segunda, la testifical, los datos no son proporcionados al tribunal directamente desde los dispositivos, sino a través de la declaración personal de quien ha tenido acceso a ellos, esto es, de quien los ha conocido directamente y transmite su contenido bajo su propia percepción. En la tercera, la pericial, y la que tratamos en un epígrafe del presente trabajo, tiene lugar mediante un informe elaborado por un técnico experto en la materia. Este técnico tendrá contacto directo con los datos originales contenidos en el dispositivo electrónico y se pronunciará al respecto desde sus conocimientos sobre la materia, en aquellos aspectos encomendados por el órgano judicial o las partes[60].

La prueba electrónica o informática contiene la información generada o transmitida a través de los dispositivos electrónicos o informáticos. Pero, además de la prueba de lo

[58] Mestre Delgado, E.: "La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos" en Figueroa Navarro. C, (directora): "La cadena de custodia en el proceso penal", Edisofer S.L, 2015, Madrid, págs.46-47.
[59] Delgado Martin, J.: "La prueba electrónica en el proceso penal", Diario La Ley, núm. 8167, octubre 2013, Madrid, págs.1-4.
[60] Ibidem, págs.47-48.

que contiene el hecho ilícito, pueden ser objeto de prueba los elementos físicos mediante los que se ha cometido el delito, es decir, los soportes informáticos: el equipo origen del hecho ilícito, servidores y nodos por los que la información, datos o archivos han circulado, los equipo y terminales finales donde la información es transmitida, recibida o transformada. En este supuesto, debido a la facilidad que tienen los equipos informáticos de ser manipulados, se adoptan las precauciones y medidas especiales para que puedan ser presentados y practicados por los tribunales como pruebas.

La prueba informática está reconocida como medio de prueba en el art. 299, apartado segundo, de la Ley de Enjuiciamiento Civil, que dice: "[…]se admitirán los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".

Por otra parte, el art. 230 de la LOPJ determina que los juzgados, tribunales y fiscalías utilicen obligatoriamente "cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones". Es decir, cuentan con instrumentos para practicar la prueba informática. Y continúa: "los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad e integridad y el cumplimiento de los requisitos exigidos por las leyes procesales".

Ahora bien, la prueba informática se considera planteada e introducida en el proceso penal como prueba documental que puede tratarse de "libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos […]" (art. 726 de la LECrim). Entendemos que una prueba informática contribuye al esclarecimiento de los hechos o a la verdad de lo sucedido. Es informática porque está en soporte electrónico. Así lo considera también el art. 26 del CP, que establece como documento "todo soporte material que expresa o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica". Atrás queda la prueba presentada en papel como soporte tradicional, ahora con la revolución tecnológica tiene cabida que se presente en soportes tecnologicos o informáticos como un audio, USB, CD, fotografía, mensajes de texto, correos electrónicos, etc. Cuando el precepto enuncia que documento es todo soporte material, entendemos que es posible presentarlo en papel o formato electrónico siempre que se refiera a hechos controvertidos, puesto que no

especifica el tipo de formato siempre y cuando favorezca a la investigación y sea relevante[61].

Según Quevedo González, son tres los elementos que componen la prueba informática[62]:

1. Soporte material: requiere su lectura o conversión a un lenguaje visual.
2. Contenido informativo: datos y hechos atribuibles a una persona.
3. Relevancia jurídica: que la información contenida acredite un hecho con trascendencia jurídica.

Como en todo procedimiento penal, es necesario que las pruebas informáticas que vayamos a introducir en el juicio cumplan una serie de requisitos. Es la LECrim quien regula expresamente la forma y garantías que deben tenerse en cuenta a la hora de practicar las diligencias de investigación tecnológica en aras de obtener la prueba correctamente y, sobre todo, el tratamiento que debe seguirse posteriormente para que ésta no se desvirtúe, es decir, mantenga su valor al reunir los requisitos de validez sustancial, procesal y formal[63].

Puesto que la prueba debe practicarse con todas las garantías, es importante comprobar que el recorrido que siguen los elementos probatorios desde su obtención o localización hasta su incorporación en el plenario han cumplido las exigencias normativas necesarias que garantizan su licitud, identidad e integridad[64].

Por ello, la prueba informática está sometida a unos requisitos de admisibilidad. Por una parte, se realiza un juicio de licitud para ver que la prueba se ha obtenido con todas las garantías procesales y respetando los derechos fundamentales sin que se produzca una violación de éstos en virtud del art. 11.1 de la LOPJ, de lo contrario, se reputarán nulas. Por otra parte, se realiza un juicio de fiabilidad, examinando la autenticidad e integridad de la prueba, es decir, que no haya sido manipulada y que conserve el contenido y que en la investigación no se hayan utilizado técnicas espurias

[61] Sanchís Crespo, C.: "La prueba en soporte electrónico" en "Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio", Thomson Reuters Aranzadi, Navarra, 2012, pág. 713.
[62] Quevedo González, J.: "Investigación y prueba del ciberdelito", Facultad de Derecho, Universidad de Barcelona, 2017, Barcelona, pág. 306.
[63] Ibidem, pág. 307.
[64] Velasco Núñez, E.: "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", El Derecho, Revista de Jurisprudencia, núm. 4, febrero, 2011, pág. 6.

para su obtención. Como hemos dicho, es relevante que se someta a este doble juicio para garantizar que es la misma que fue incautada o aprehendida[65].

I) Juicio de licitud

Para que una prueba sea válida tiene que haberse obtenido sin violar los derechos fundamentales, como enuncia el precepto que hemos mencionado anteriormente. La ilicitud de una prueba puede desencadenar que otras derivadas o reflejas de aquella queden anuladas si entre éstas existiera una conexión natural o causal. Ningún elemento probatorio derivado de un hecho vulnerador de un derecho fundamental puede valorarse si entre ese elemento y el hecho existe un nexo causal, es decir, que de no haberse producido ese hecho no hubieran tenido lugar dichos elementos. Esto permite afirmar que la ilegitimidad de las primeras se extiende a las segundas.

Dado que, en este trabajo, hemos estudiado al agente encubierto en el capítulo anterior, los requisitos para la licitud de la prueba obtenida por éste son que su intervención se haya producido con autorización judicial y que se trate de determinados delitos. Sin embargo, es preciso aclarar que, aparte del agente encubierto como técnica de investigación para los ciberdelitos, contamos con la interceptación telefónicas y telemáticas, el registro de dispositivos de almacenamiento de información y el registro remoto de equipos informáticos, los cuales no han sido objeto de estudio en este trabajo pero consideramos necesario mencionarlos, puesto que, aunque sean técnicas más gravosas que las del agente encubierto informático, también tienen utilidad y cabida dentro de la lucha contra la ciberdelincuencia.

En consecuencia, la falta de licitud provoca la nulidad de la prueba por haberse obtenido con violación del derecho a la intimidad personal del encausado, secreto de las comunicaciones o la protección de datos, todos ellos recogidos en el art. 18 de la CE. Esta nulidad conlleva la carencia de eficacia probatoria[66]. Es importante, a su vez, mencionar que la cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos puede quedar viciada desde el momento en que las FYCS, acceden a los vestigios de manera directa y sin autorización judicial, dado que se trata de dispositivos que contienen o transmiten datos vinculados a los derechos fundamentales expuesto anteriormente[67].

[65] Quevedo González, J: "Investigación y prueba del…", op. cit., pág.308.
[66] Ibidem, págs. 309-312.
[67] Mestre Delgado, E.: "La cadena de custodia…", op. cit., pág. 50.

II) Juicio de fiabilidad

Hemos dicho que la fiabilidad se refiere a que la prueba sea auténtica e íntegra. Para su comprobación, se somete a este juicio, de forma que no haya dudas respecto a las técnicas a través de las cuales se hayan obtenido, que no se traten de técnicas espurias y que se contrasten con la finalmente aportada en el juicio. Para que la prueba no sea manipulada es importante garantizar lo que se denomina cadena de custodia, de manera que no se pierda ningún eslabón y pueda presentarse la prueba tal como se halló. En palabras de Mestre Delgado, la cadena de custodia es "una sucesión de fases procedimentales que deben estar interconexionadas entre sí". Mestre Delgado explica que es fundamental la existencia de una concatenación de actuaciones, es decir, que cada actuación arranque de la anterior y concluya en la siguiente, sin interrupciones que alteren esa vinculación interna. Para asegurarnos de que la prueba presentada ha sido protegida por la cadena de custodia, y evitar procedimientos impugnatorios contra aquella, la doctrina recomienda a los funcionarios o peritos, añadir en sus atestados o informes, una referencia sobre los eslabones de la cadena de custodia previo y posterior a su intervención. Este hecho proporcionará mayor seguridad llegado el juicio oral, pues será más difícil que haya lugar a descalificaciones del contenido de las actuaciones policiales basándose en la falta de acreditación del efectivo cumplimiento del protocolo de cadena de custodia[68]. Además, con este juicio se pretende analizar la veracidad de la prueba. En otras palabras, se trata de evitar la manipulación, falsedad, distorsión e imitación del material informático objeto de prueba[69].

El punto débil del material informático es que es fácilmente manipulable sin apenas dejar rastro. Por ello, las autoridades policiales tienen la tarea de cumplir fielmente con los procedimientos transparentes y seguros que les permitan obtener las pruebas manteniendo su integridad, autenticidad y confiabilidad[70].

Cualquier duda que pueda tenerse sobre la fiabilidad, autenticidad e integridad de aquélla generará como regla general su inadmisibilidad en el proceso. Así, el juez examinará la fuente de la prueba informática, es decir, examinará la fiabilidad del registro material de prueba, pero además deberá comprobar la fiabilidad del procedimiento llevado a cabo para su preservación, y las garantías que han asegurado ese mantenimiento

[68] Ibidem, págs.69-70.
[69] Quevedo González. J: "Investigación y prueba del…", op. cit., pág. 313.
[70] Roviera Del Canto, E.: "Tratamiento penal sustantivo de la falsificación informática", Cuadernos de Derecho Judicial, núm.10,2001, págs. 477-478.

de cualquier elemento probatorio, y si el material presentado es el mismo que el incautado o aprehendido desde el principio del proceso de diligencias previas[71]. El procedimiento al que hacemos referencia no es otro que el de cadena de custodia, que además de garantizar la identidad del objeto, también acredita su autenticidad, es decir, asegura que la prueba no ha sido manipulada o alterada.

En relación con las pruebas que recaba el agente encubierto informático, para que estas sean fiables es necesario determinar[72]:

- El canal cerrado de comunicación al que se ha accedido.
- La forma de acceso al canal de comunicación.
- El tipo de archivo ilícito que se tiene intención de enviar o intercambiar.
- El destino y uso de esos archivos ilícitos en la red.

Por último, pero no menos importante, otro medio que refuerza la fiabilidad de la prueba informática es el código *hash*. Gracias a él es posible controlar los archivos ilícitos intercambiados debido a que la Policía Judicial los almacenará y auditará en unos ficheros cuyas bases de datos sean seguras, y cada uno contendrá dicho código para evitar cualquier posible manipulación por parte de terceros sobre los mismos[73].

En consecuencia, la falta de confiabilidad no da lugar a la nulidad, pero disminuye el valor probatorio. Un buen juicio de fiabilidad abarca desde la forma de obtención de la prueba, los medios empleados para ello, hasta el procedimiento que se ha seguido para obtenerla. En otras palabras, el juicio de fiabilidad controla la veracidad de lo que se va a presentar como prueba y nos permite comprobar que se ha obtenido respetando las medidas de seguridad que garantizan la integridad, autenticidad, confidencialidad, calidad, protección y conservación de la información. En definitiva, con él vemos si se ha cumplido el protocolo a seguir en estos supuestos de forma que la información no resulte manipulada ni se pierda rastro de ésta[74].

2. Modos de certificación y presentación de la prueba

La forma de presentar la prueba en los ciberdelitos cambia radicalmente de la forma en que se presentan las que están relacionadas con delitos físicos. Ahora es necesario

[71] Quevedo González, J.:" Investigación y prueba del…", op. cit., pág. 314.
[72] Ibidem, págs. 344-345.
[73] Rubio Alamillo, J: "La informática en la reforma de la Ley de Enjuiciamiento Criminal", Diario La Ley, 10 de diciembre de 2015, pág. 9.
[74] Quevedo González, J.: "Investigación y prueba del…", op. cit., pág. 345.

certificarlas antes de su presentación. En otras palabras, si queremos presentar una prueba informática en el proceso judicial, deberá practicarse una prueba pericial, descartándose la opción de presentar la prueba mediante "pantallazos", impresiones, etc. La presentación de pantallazos o impresiones de correos electrónicos, conversaciones de WhatsApp o contenido de redes sociales, serán impugnadas porque no ha intervenido ningún medio o técnica que garantice su autenticidad.

Otro aspecto para tener en cuenta a la hora de certificar una prueba es la presencia de un perito informático en lugar de un notario, ya que éste no puede desarrollar las funciones competentes al perito, principalmente porque así lo prohíbe el art. 199 del Reglamento de la organización y régimen del notariado, que imposibilita a un notario actuar allí donde sean precisos conocimientos periciales. El notario podrá dar fe de que unos mensajes de WhatsApp o de correo electrónico pueden encontrarse en determinados soportes o determinado mensaje en alguna red social se encuentra publicado, pero no garantizar su autenticidad e integridad. Esto es importante señalarlo, pues recientemente los notarios han puesto de moda realizar actas notariales para testimoniar mensajes de aplicaciones de mensajería instantánea, de correos electrónicos o de contenido de Internet. Sin embargo, no pueden garantizar la autenticidad ni integridad de éste bajo el precepto señalado anteriormente, en ningún supuesto, por eso el acta notarial no puede utilizarse en teoría por la vía policial o judicial[75].

Otro modo de certificar la prueba informática es a través de prestadores de servicios electrónicos de confianza, los anteriormente conocidos como Terceros de confianza que contemplaba el art. 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y que han quedado derogados. Se trata fundamentalmente de servicios de entrega electrónica certificada y de conservación de firmas y sellos electrónicos, amparados por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Por ejemplo, *eGarante* es un Prestador de Servicios de Confianza no cualificado inscrito en el registro de prestadores del Ministerio de Industria, consciente de la volatilidad de la información en Internet. Por ese motivo ha desarrollado una solución

[75] Rubio Alamillo, J.: "Adquisición y presentación en un procedimiento judicial de una prueba informática", Lefebvre, El Derecho, abril, 2017, pág. 3. Visto el 6 de diciembre de 2020 en web: https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica

tanto para empresas como para particulares, creando una herramienta para probar la existencia de lo que vemos, enviamos y recibimos por Internet.

Las certificaciones emitidas por eGarante son una prueba en documento privado que se aporta con la intervención de un tercero independiente ajeno a la controversia con unas solidas cualidades en su obtención desde el punto de vista pericial, debido a que ha sido obtenido sin manipulación por la parte que aporta la prueba y con la "cadena de custodia" reforzada. Para garantizar la no manipulación se sigue un proceso pericialmente sólido y aplicando unos métodos criptográficos que tienen como finalidad asegurar la cadena de custodia desde que se crea la prueba por parte de eGarante hasta que se presenta y valora en los juicios. eGarante puede emitir la certificación de la URL de una página de Internet o Red Social, pasando por correos electrónicos y los documentos adjuntos. De forma que se garantiza la integridad del contenido y la identidad del testigo tercero independiente que lo acredita.

Gracias a su proceso técnico, en el que un tercero valida el momento en el que se produce la comunicación electrónica, demuestra que los datos han existido y no se han modificado desde un momento concreto en el tiempo. Además, el documento original creado por eGarante puede validarse para verificarse la autenticidad e integridad en la web del Ministerio de Industria. En este sentido, podremos validar la firma de eGarante, imprimir el resultado y añadirlo a la prueba como resultado de aplicar el proceso de validación de firmas a la certificación emitida por la plataforma[76].

Otro ejemplo, es *SafeStamper*. Se trata también de una plataforma cuya finalidad es la certificación digital, generación de evidencias electrónicas para acreditar el contenido e información existente en Internet, redes sociales, correos electrónicos, fotografías, videos y audios hechos con *smartphones*, incluyendo su ubicación, o cualquier otro contenido[77].

Hay dos sentencias relevantes sobre la aportación de conversaciones en redes sociales, que permiten dilucidar si tiene cabida o no este tipo de servidores como material probatorio. Siguiendo esta línea, encontramos la STS 2047/2015, dictada por la Sala de lo Penal, sección 1ª, en fecha 19 de mayo de 2015, donde menciona que una captura de pantalla sin más no es suficiente como prueba de publicaciones en redes sociales y dice

[76] Egarante: https://www.egarante.com/, visto el 2 de diciembre de 2020.
[77] SafeStamper: https://www.safestamper.com/products, visto el 1 de diciembre de 2020.

en su página seis que la carga de la prueba corresponde a quien pretende aprovechar la idoneidad probatoria, requiriendo una prueba pericial: “De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido”.

La segunda STS es la 2949/2018, dictada por la Sala de lo penal el 19 de julio de 2018, e indica que no es imprescindible la prueba pericial cuando “no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba”. Y, concretamente, en su página seis menciona a la STS 755/2015, que recoge: “No es posible entender, como se deduce del recurso, que estas resoluciones establezcan una presunción iuris tantum de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; sino que, en el caso de una impugnación (no meramente retórica y en términos generales) de su autenticidad -por la existencia de sospechas o indicios de manipulación- se debe realizar tal pericia acerca del verdadero emisor de los mensajes y su contenido. Ahora bien, tal pericia no será precisa cuando no exista duda al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba”.

Por otros medios de prueba entendemos que pueden ser, por ejemplo, las dos herramientas comentadas anteriormente, que validan la autenticidad e integridad del contenido que se pretende presentar como prueba, y por ello no sería necesaria una pericial informática.

¿Cómo debemos presentar una prueba informática en un procedimiento judicial?

- Si se trata de un correo electrónico, un fichero informático, una URL de página web donde se encuentra el contenido que corrobora el presunto delito, etc., la prueba deberá presentarse siempre en formato digital. Cabe la posibilidad de presentarla también en formato papel para mayor comodidad de los abogados, fiscales y jueces; sin embargo, la prueba deberá incluirse en soporte informático, óptico (CD, DVD) o magnético (Disco duro, memoria USB). En este último caso es imprescindible que, para que sea válida, se realice una duplicación ante notario

del soporte y obtener el código *hash* de aquél, que garantiza la no manipulación del contenido en el mismo, y será anotado en el acta notarial.

- Si se trata de una información volátil, que puede desaparecer con una acción humana en cualquier momento (por ejemplo, unas fotografías, vídeos o comentarios ofensivos en alguna red social o página web, una noticia, etc.), la elección más idónea para presentarla en un juicio es certificarla mediante un notario digital y, si las circunstancias informáticas no lo permitieran, tiene cabida la intervención de un notario tradicional que será orientado bajo las directrices del perito informático. Si nos decantamos por los notarios digitales, también conocidos como Terceros de Confianza, será necesario que, como dichos prestadores de servicios, cumplan con la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y con los requerimientos de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Igualmente, las empresas que oferten estos servicios deberán cumplir con los estándares establecidos por las normas ISO. La forma de conocer que el notario digital o tercero de confianza tiene la madurez tecnológica adecuada y cumple con toda la normativa técnica y legal, que evite posteriormente una posible impugnación de la prueba, es contratando un perito informático colegiado que dirija el proceso de certificación de las evidencias que van a revelarse.
- Si se trata de pruebas obtenidas a partir de dispositivos móviles, necesitaremos realizar un volcado forense de aquéllas usando herramientas tipo de mercado. Entre éstas destaca *Cellebrite UFED Touch*, utilizada por la Guardia Civil y el CNP, para investigar delitos de organizaciones criminales[78].

3. Prueba pericial informática

La prueba pericial informática tiene como objetivo analizar los dispositivos electrónicos que ha incautado la Policía y que se encuentran a disposición de la Autoridad Judicial en un procedimiento penal. En ocasiones, ese principal fin se complementa con

[78] Rubio Alamillo, J.: "Adquisición y presentación en un procedimiento judicial de una prueba informática", Lefebvre, El Derecho, abril 2017, págs. 4-6, visto el 6 de diciembre de 2020 en https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica

otro: determinar la autoría del ataque o la intención con la que se ha cometido[79]. Por tanto, tiene dos funciones: por un lado, refuerza la fiabilidad de la prueba, puesto que es examinada por las autoridades y expertos competentes, garantizando la integridad y autenticidad de la información y, por otro lado, sirve para investigar quién o quiénes están detrás de la comisión del ciberdelito[80].

El propósito de la prueba pericial dependerá de lo que se quiera investigar, que va desde:

- Analizar si un software es o no original o si la copia está autorizada.
- Analizar los canales de comunicación mediante los cuales ha tenido lugar el ciberdelito en concreto y dónde se originó y cuál fue su destino.
- Recuperación de archivos ocultos, encriptados o eliminados.
- Cualquier otro fin que exija la investigación.

Los sujetos que realizarán las pruebas periciales informáticas autorizadas por un auto serán[81]:

- Grupo de Delitos Telemáticos de la Guardia Civil
- Brigada de Investigación Tecnológica de la Policía Nacional o los departamentos especialistas de la Policía Autonómica correspondiente.
- Expertos como ingenieros informáticos o técnicos en informática.
- Se plantea la posibilidad de que la policía realice pruebas periciales sin necesidad de la intervención de un juez que dicte el auto para ello, sin que ese hecho afecte a la eficacia procesal y a la validez de la prueba pericial informática. La jurisprudencia ha resuelto esta cuestión pronunciándose a favor de que la policía practique la pericial sin necesidad de existencia de mandato judicial que ordene a los expertos a ello, salvo que la práctica de la pericial afecte a los derechos fundamentales; todo ello en virtud del art. 11.1 de la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad del Estado, que atribuye expresamente a los cuerpos policiales la facultad de "investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del juez o tribunal competente y elaborar los informes

[79] Velasco Núñez, E: "Delitos cometidos a través de Internet: cuestiones procesales", Ed. La Ley,2010, Madrid, págs.238-240.
[80] Quevedo González, J.: "Investigación y prueba del…", op. cit., págs.352-353.
[81] Ibidem, págs. 348-349.

técnicos y periciales procedentes". En este sentido, la STS 179/2006, de 14 de febrero, estableció que "la intervención del juez, salvo en supuestos de afectación de derechos fundamentales, no debe impedir la posibilidad de actuación de la policía, en el ámbito de la investigación y averiguación de los delitos en los que posee espacios de actuación autónoma".

- Técnicos informáticos de un organismo oficial perjudicado por el delito siempre bajo el conocimiento de las partes por si tuvieran que ejercitar la recusación en caso de concurrir alguna de las causas legales para ello (arts. 416, 464 y 468 LECrim).

No está de más explicar brevemente que la LECrim en su art. 457 establece que los peritos titulados en la materia objeto del dictamen son considerados peritos titulares, mientras que aquellos que no lo son se les considera peritos no titulares. Siguiendo esta línea, encontramos que los ingenieros informáticos, desde nuestro punto de vista, son los más indicados para analizar una prueba de un presunto ciberdelito. Estos no se encuentran regulados en España, por ende, en la actualidad existen numerosos profesionales que se denominan peritos informáticos, los cuales, aunque carecen de título oficial, tienen conocimiento o práctica en la materia.

Respecto a la presentación y práctica de la prueba pericial, si no podemos reproducir el acto pericial en el juicio oral, podrá tener lugar la recusación tal como indica el art. 467 de la LECrim, y en ese caso, cada parte acudirá con su representante y será el juez quien dictamine las precauciones oportunas (art. 476 LECrim). Por tanto, una vez que el juez determine que procede una prueba pericial, y puesta en conocimiento de las partes personadas, será la parte interesada quien solicite la asistencia a la práctica de la pericia. Al acto pericial asistirá el Letrado de la Administración de Justicia que actúe en la causa (art. 477 LECrim). La personación del LAJ aporta validez probatoria. También cabe la posibilidad de que se practique como prueba anticipada a propuesta de las partes si prevén que no va a poder practicarse en juicio oral o va a ser causa que motive su suspensión[82].

Durante la fase de instrucción, las partes personadas en el acto pericial podrán incrementar sus facultades de participación con el pronunciamiento de sus observaciones sin perjuicio de que logren contradecir e interrogar sobre ella los peritos, o de contribuir

[82] Quevedo González, J.:" Investigación y prueba del ciberdelito…", op. cit., pág. 354.

una contra pericia propia o similar. Todas las pericias que se practiquen deben reflejarse en un informe pericial (art. 478 LECrim), el cual contendrá los siguientes puntos: descripción del objeto, una lista de todas las acciones practicadas y su efecto, asimismo las conclusiones que ha formulado el perito conforme a los principios y reglas de su disciplina.

En el juicio oral, el Ministerio Fiscal y las partes manifestarán en los escritos de calificación las pruebas de las que se van a valer y se practicarán aquellas que hayan sido pedidas por las partes y declaradas pertinentes por el órgano judicial. Sin embargo, el juez podrá practicar las diligencias de prueba de oficio, sin que hayan sido propuestas, siempre que las considere necesarias para comprobar los hechos recogidos en los escritos de calificación (art. 729.2 LECrim). En el juicio ordinario, queda a decisión del juez la posibilidad de acordarla si la considera necesaria para comprobar algún hecho objeto de los escritos de calificación (art. 729.2 LECrim). En el juicio abreviado, las partes pueden proponerla al principio del juicio oral y la práctica se hace en el juicio oral salvo que se haya pedido prueba anticipada o preconstituida. En tales casos, se aportará como prueba documental y será evaluada en la sentencia, sin necesidad de que el perito se ratifique en el juicio. Por otro lado, si alguna de las partes lo impugnara en el escrito de conclusiones, deberá estar presente el perito para someterse a contradicción (STS 1281/2006, de 27 de diciembre)[83].

Cuando las partes son quienes incorporan las pruebas informáticas al proceso, en la gran mayoría de veces, las acompañan de un dictamen pericial informático para dar mayores datos al juzgado de forma que éste pueda valorar la actividad presuntamente ilícita y fundamentar la petición de diligencias de investigación que suelen ordenarse cuando se recibe una denuncia o querella o posteriormente tras la incoación del procedimiento.

La prueba pericial puede atender a la posible ilicitud o nulidad de ésta, cuando, lejos de un control por parte del juzgado, afecte a los derechos fundamentales. Recordemos que, al tratarse de ciberdelitos, en la gran mayoría habrá que analizar datos de carácter personal, vinculados con la esfera personal o al contenido de sus comunicaciones, pudiendo surgir una confrontación entre investigar el delito y realizar una pericia del objeto del delito o a través del cual se ha cometido. El resultado de vulnerar

[83] Ibidem, págs. 354-355.

los derechos fundamentales nombrados anteriormente y recogidos en el art. 18.1, 3 y 4 de la CE, conlleva la nulidad plena y directa de la pericia. Otro de los puntos débiles es acreditar que el objeto de prueba pericial no ha sido manipulado ni alterado, puesto que aún no se ha contado con la intervención judicial o policial que garantice la labor de conservación[84].

CONCLUSIONES

Se ha comprobado, tras el análisis del tema, que los cambios de vida y de ritmo que la sociedad experimenta constantemente llevan aparejados el surgimiento de nuevas formas de comisión delictivas, en este caso, sirviéndose de las TIC y la red de Internet por parte de los delincuentes, dadas las características de aquéllas que favorecen su aparición, creando oportunidades para delinquir y naciendo así el fenómeno de la Ciberdelincuencia, la cual ha tenido que ser regulada desde un plano internacional, dado su carácter transnacional, y traspuesta con posterioridad a los ordenamientos jurídicos de aquellos países que se han adherido al instrumento regulatorio más destacado en este ámbito: el Convenio de Budapest. Siguiendo esta línea, y tras estudiar el Convenio, no podemos dejar pasar por alto la necesidad de su modificación, puesto que se trata de un instrumento jurídico pretérito que adolece de la ausencia de ciertas categorías de ciberdelitos que se cometen en la actualidad. Por ello, vemos necesario una reforma de éste en aras de proteger correctamente los bienes jurídicos y aumentar la seguridad jurídica en el marco de la informática y telecomunicaciones.

Sin embargo, nuestro ordenamiento jurídico en relación con la ciberdelincuencia ha sabido manejar la situación, llevándose a cabo varias reformas para incluir nuevas conductas antijurídicas. Nuestro legislador ha sido consciente de que las TIC van un paso por delante del Derecho Penal, lo que conlleva estar en continuo estudio y cambio.

No obstante, hemos observado que, pese a que las conductas delictivas se encuentran tipificadas, las penas correlativas a ellas nos parecen poco idóneas, en cuanto a que los delitos tratados en este trabajo afectan sobre todo a la esfera personal y patrimonial, que consideramos de especial relevancia por el trasfondo que guardan, y cuyas penas no son lo suficientemente altas.

[84] Ibidem, págs. 368-369.

La realidad es que, después de comprender nuestro ordenamiento, quisimos investigar sobre las herramientas de investigación procesal-penal con las que cuenta para investigar y perseguir a los ciberdelitos como a sus autores, dando con la figura del agente encubierto informático, que a diferencia del agente encubierto físico que conocíamos, nos revela unas mayores ventajas, como, por ejemplo, su peculiaridad de actuar en canales cerrados, o la de actuar e intervenir siempre mediante una resolución dictada por el juez instructor del proceso. Se trata de una técnica de investigación que no agrede los derechos fundamentales de los investigados tanto como pudieran hacerlo otras.

La ciberdelincuencia se ha visto reforzada por los elementos mencionados anteriormente, y sigue habiendo un punto débil: la dificultad de probar el ciberdelito, unida a su obtención y práctica de la misma. De ello deducimos que queda trabajo aún por hacer, puesto que, aunque sean admitidas las pruebas informáticas en el ámbito jurídico, la LECrim no es tan explícita a la hora de indicar la forma de presentarlas ni el modo de garantizar su licitud e integridad, teniendo que recurrir a lo que dicta la jurisprudencia del alto tribunal.

Cabe destacar, en consecuencia, que la Ciberdelincuencia continua siendo a día de hoy un asunto sobre el que seguir estudiando y trabajando, pues no paran de incrementarse los casos por ciberdelitos y, aunque existan normativas reguladoras, herramientas contra su lucha y procedimientos procesales más concretos para su investigación y enjuiciamiento, continúa siendo uno de los puntos dentro del Derecho Penal en constante cambio, y que debemos prevenir en aras de proteger los bienes y derechos de las personas que conforman nuestra sociedad.

BIBLIOGRAFÍA

ABADÍAS SELMA. A.: “El peligro de la sobreexposición de los menores a internet frente al *child grooming* en tiempos del covid-19”, La Ley Penal, Ed.Wolters Kluwer, núm.144, mayo-junio, 2020.

ACURIO DEL PINO, S.: “Delitos informáticos: generalidades”, Organización de los Estados Americanos, 2017. Visto en web: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

ALCOLADO CHICO, M.ª T.: "La evolución hacia la moderna funcionalidad del agente encubierto: incidencia de las nuevas reglas de la Ley de Enjuiciamiento Criminal", Revista Jurídica de Asturias, núm. 39, noviembre, 2016.

ALONSO DE ESCAMILLA, A.:" El delito de stalking como nueva forma de acoso. Cyberstalking y nuevas realidades", La Ley Penal, Ed. Wolters Kluwer, núm.105, noviembre-diciembre, 2013.

ÁLVAREZ RODRÍGUEZ, I.: "El derecho del ciberespacio: una aproximación", Revista de Internet, Derecho y Política, núm. 30, marzo, 2020.

BARRIO ANDRÉS, M.:

- "Delitos 2.0: Aspectos Penales, Procesales y de Seguridad de los Ciberdelitos", Ed. Wolters Kluwer, Madrid, 2018.
- "Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010", La ley penal, Ed. Wolters Kluwer, núm.86, octubre, 2011.
- "Ciberdelitos: Amenazas criminales del ciberespacio", Ed. Reus, Madrid, 2017.

CEREZO DOMÍNGUEZ, A.I: "La ciberdelincuencia en España: un estudio basado en las estadísticas policiales", Revista electrónica de estudios penales y de la seguridad, núm.6, abril, 2020.

DE LA MATA, J.: "El agente encubierto online", Congreso Internacional "la Nueva Reforma Procesal Penal": Derechos Fundamentales e Innovaciones Tecnológicas, Organizado por el Ministerio de Ciencia y Tecnología y Vicente Gimeno Sendra, coord. del Máster Universitario de Derechos Fundamentales en la UNED, Facultad de Derecho de la UNED, 17 de octubre de 2017, visto en web: https://canal.uned.es/video/5a6f55f0b1111f655c8b45a8

DELGADO MARTÍN, J.:

- "Medios encubiertos de investigación de la criminalidad organizada", Actualización de la 2ª parte de "La criminalidad organizada", 2017, visto en web: https://n9.cl/95bbn.
- "La prueba electrónica en el proceso penal", Diario La Ley, núm. 8167, octubre, 2013, Madrid.

DE URBANO CASTRILLO, E.: “Los delitos informáticos tras la reforma del CP de 2010”, Revista Aranzadi Doctrinal, núm.6, octubre, 2011.

DIAZ GÓMEZ, A.: “El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest”, REDUR, núm.8, diciembre, 2010.

ESPINOSA SÁNCHEZ, J.F.: “Ciberdelincuencia. Aproximación Criminológica de los delitos en la red”, La Razón Histórica, núm.44, septiembre-diciembre, 2019.

FANJUL, FERNÁNDEZ, M.ª. L.: “Conceptualización, evolución y clasificación del ciberdelito empresarial”, Ed. AMEC Ediciones, Madrid, 2018.

FLORES PRADA, I.: “Criminalidad informática. Aspectos sustantivos y procesales”, Ed. Tirant lo Blanch, Valencia, 2012.

GALÁN MUÑOZ, A.: “Los ciberdelitos en el ordenamiento español”, Ed. UOC S.L, Barcelona, 2019.

GIL GIL, A. y HERNÁNDEZ BERLINCHES, R.: “Cibercriminalidad”, Ed. Dykinson, Madrid, 2019.

GÓMEZ HERNÁNDEZ, J.A. y RAYÓN BALLESTEROS, M.ª. C.: “Cibercrimen: particularidades en su investigación y enjuiciamiento”, Anuario Jurídico y Económico Escurialense, núm. 47, 2014.

GONZÁLEZ GARCÍA, A. y GIRAO GONZÁLEZ, F.J.: “Capacidades prospectivas y de defensa en la lucha contra el ciberterrorismo: análisis del caso español”, Revista de Relaciones Internacionales, Instituto de Relaciones Internacionales, UDIMA, núm. 58, junio, 2020, Madrid.

GONZÁLEZ GARCÍA, S.: “El agente encubierto informático a examen: un análisis de su regulación y de la validez de su actividad investigadora y probatoria en el proceso penal”, La Ley Penal, Ed. Wolters Kluwer, núm.139, julio-agosto, 2019, Madrid.

GONZÁLEZ HURTADO, J. A.: “Delincuencia informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma”, tesis doctoral, Universidad Complutense de Madrid, Madrid, 2013.

HERNÁNDEZ DIAZ, L.: “El delito informático”, Eguzkilore, núm. 23, San Sebastián, diciembre, 2009.

HESS ARAYA.C.: “Ciberdelitos: tipos y soluciones” en “Ciberseguridad en Costa Rica”, Programa Sociedad de la Información y el Conocimiento Universidad de Costa Rica, San José, octubre, 2010.

MAGAZ ALVAREZ, R.: “Criminalidad y Globalización. Análisis y estrategias ante grupos y organizaciones al margen de la ley”, Ed. Instituto Universitario General Gutiérrez Mellado, Madrid, 2016.

MARTÍN ME, A.M.: “Estafas informáticas: tipificación y cuestiones técnico-jurídicas”, Unidad Didáctica obtenida del Máster Penal Económico de la Universidad Rey Juan Carlos, Facultad de Derecho, Madrid, 2019.

MARTÍNEZ SÁNCHEZ, M.T.:

- “Incidencia de la última reforma del Código Penal por LO 1/2015, de 30 de marzo, en materia de violencia de género. Especial referencia a la agravante de género y a los nuevos delitos de stalking y sexting.”, El Derecho, Ed. Lefebvre, noviembre, 2016, visto en web: https://elderecho.com/incidencia-de-la-ultima-reforma-del-codigo-penal-por-lo-12015-de-30-de-marzo-en-materia-de-violencia-de-genero-especial-referencia-a-la-agravante-de-genero-y-a-los-nuevos-delitos-de-stalking-y-sex
- “El acceso a menores con fines sexuales a través de las TIC: delito online child grooming y embaucamiento de menores, tras la reforma del CP por la LO 1/2015”, El Derecho, Ed. Lefevre, abril, 2017.

MESTRE DELGADO, E.: “La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos”, en FIGUEROA NAVARRO (directora) La cadena de custodia en el proceso penal, Ed. Edisofer, Madrid, 2015.

MIRÓ LLINARES, F.: “El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio”, Ed. Marcial Pons, Madrid, 2013.

NÚÑEZ PAZ M.A. y GUILLÉN LÓPEZ, G.: “Entrega vigilada, agente encubierto, y agente provocador. Análisis de los medios de investigación en materia de tráfico de drogas”, Anuario de Derecho Penal y Ciencias Penales, Ministerio de Justicia, vol. 61, 2008.

PANIZO GALENDE, V.: “El ciber-acoso con intención sexual y el child-grooming”, Cuadernos de criminología: revista de criminología y ciencias forenses, núm.15, 2011. Visto en web: https://fliphtml5.com/fgec/iizr/basic

PALOP BELLOCH, M.: “Las medidas de investigación tecnológica”, Revista de derecho procesal, núm. 2, diciembre, 2017.

PÉREZ GÓMEZ, A.: “Ciberterrorismo, ¿una nueva amenaza?”, Instituto Español de Estudios Estratégicos, núm.19, septiembre,2020.

PONS GAMÓN, V.: “Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad”, URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, Ecuador, julio,2017.

PORTA FRUTOS, C.: “El ánimo de lucro en la defensa penal de los derechos de autor”, The Law Clinic, ECIJA, febrero, 2019. Visto en web: https://ecija.com/el-animo-de-lucro-en-la-defensa-penal-de-los-derechos-de-autor/

PUYOL, J.: “¿Qué es y en qué consiste el sexting?”, agosto, 2020. Visto en web: https://confilegal.com/20200817-que-es-y-en-que-consiste-el-sexting/

QUEVEDO GONZÁLEZ, J.: “Investigación y prueba del ciberdelito”, Universidad de Barcelona, Programa de Doctorado en Derecho y Ciencia Política, Facultad de Derecho, Universidad de Barcelona, Barcelona, 2017.

RODRÍGUEZ BERNAL, A.: “Los cibercrímenes en el espacio de libertad, seguridad y justicia”, Revista de Derecho Informático, núm. 103, septiembre, 2007.

RODRÍGUEZ-VÁZQUEZ, V.: “Los ciberdelitos contra la propiedad intelectual ¿cambiar todo para que nada cambie?: del ánimo de lucro al de obtener beneficio económico directo o indirecto”, Revista electrónica de ciencias criminológicas, Universidad de Vigo, núm. 4, Zenbakia, 2019.

ROVIERA DEL CANTO, E.: “Tratamiento penal sustantivo de la falsificación informática”, Cuadernos de derecho judicial, núm.10, Madrid, 2001.

RUBIO ALAMILLO, J.: “Adquisición y presentación en un procedimiento judicial de una prueba informática”, El Derecho, Ed. Lefevre, abril, 2017. Visto en web: https://elderecho.com/adquisicion-y-presentacion-en-un-procedimiento-judicial-de-una-prueba-informatica

SÁNCHEZ CANET, F.J.: "Cibercriminalidad especial referencia al delito de usurpación y suplantación de identidad", UNIR, Trabajo de Fin de Máster, Valencia, 2016.

SÁNCHEZ GÓMEZ, R.: "Agente encubierto informático en la ciberdelincuencia", La Ley Penal, Ed. Wolters Kluwer, núm.118, enero-febrero, 2016.

SANCHÍS CRESPO, C.: "La prueba en soporte electrónico en las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio", Ed. Thomson Reuters Aranzadi, Navarra, 2012.

SESMA DEL VAL, O.: "El estudio de un concurso de delitos de detención ilegal, lesiones, injurias, amenazas y daños", Facultad de Derecho de Zaragoza, Trabajo de Fin de Máster, núm. 201, Zaragoza, 2019.

SOLANO DE CASTRO. S: "El Agente Encubierto Informático", Universidad Complutense, Facultad de Derecho de Madrid, Trabajo Fin de Máster, Madrid, 2020.

TEMPERINI, M.: "Delitos informáticos y cibercrimen: alcances, conceptos y características" en "Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de Internet", Ed. Erreius, Buenos Aires, 2018.

VALLÉS CAUSADA, L.: Tecnología aplicada por la Policía a la investigación criminal, "Congreso internacional: la nueva reforma procesal penal: Derechos fundamentales e Innovaciones Tecnológicas", Organizado por el Ministerio de Ciencia y Tecnología y Vicente Gimeno Sendra, coord. del Máster Universitario de Derechos Fundamentales en la UNED, Facultad de Derecho de la UNED, octubre, 2017, visto en la web: https://canal.uned.es/video/5a6f55edb1111f655c8b458e

VELASCO NÚÑEZ, E.:

- "Los delitos informáticos", Sepín Editorial Jurídica, núm. 81, diciembre, 2015.
- "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", Revista de Jurisprudencia, El Derecho, núm.4, febrero,2011.
- "Delitos cometidos a través de Internet: cuestiones procesales", Ed. La Ley, Madrid, 2010.

VIVÓ CABO, S.: "La globalización del delito: ciberdelincuencia", La Ley Penal, núm.132, 2018.

ZARAGOZA TEJADA, J.I.: "El Agente Encubierto Online". En: Bermúdez González, J.A., García Marcos, J., Perals Calleja, J., Tejada de la Fuente, E., Velasco Núñez, E., Zaragoza Aguado, J.A., Investigación Tecnológica y Derechos Fundamentales: Comentarios a las modificaciones introducidas por la Ley 13/2015, Ed. Thomson Routers, Navarra, 2017.

PÁGINAS WEBS CONSULTADAS:

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática: https://www.mpr.gob.es/Paginas/index.aspx

Egarante:

https://www.egarante.com/

SafeStamper:

https://www.safestamper.com/products

LEGISLACIÓN

- Consejo de Europa. Convenio sobre la ciberdelincuencia, 23 de noviembre de 2001, núm.185.
- Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm.311.
- Instrumento de ratificación de la Convención de las Naciones Unidas contra el tráfico ilícito de estupefacientes y sustancias sicotrópicas, hecha en Viena el 20 de diciembre de 1988. Boletín Oficial del Estado, 10 de noviembre de 1990, núm.270.
- Instrumento de Ratificación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Nueva York el 15 de noviembre de 2000. Boletín Oficial del Estado, 29 de septiembre de 2003, núm. 233.
- Instrumento de ratificación de la Convención de las Naciones Unidas contra la corrupción, hecha en Nueva York el 31 de octubre de 2003. Boletín Oficial del Estado, 19 de julio de 2006, núm.171.

- Instrumento de Ratificación del Convenio del Consejo de Europa sobre la protección de niños contra la explotación y el abuso sexual, hecho en Lanzarote el 25 de octubre de 2007. Boletín Oficial del Estado, 12 de noviembre de 2010, núm.274.
- Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado, 17 de septiembre de 2010, núm.226.
- Instrumento de Ratificación del Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003.Boletín Oficial del Estado, 30 de enero de 2015, núm.26.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm.281.
- Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando. Boletín Oficial del Estado, 13 de diciembre de 1995, núm.297.
- Ley Orgánica 2/86, de 13 de marzo, sobre Fuerzas y Cuerpos de Seguridad. Boletín Oficial del Estado, 14 de marzo de 1986, núm.63.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Boletín Oficial del Estado, 6 de diciembre de 2018, núm. 294.
- Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. Boletín Oficial del Estado, 13 de enero de 2000, núm.11.
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Boletín Oficial del Estado, 2 de julio de 1985, núm.157.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Boletín Oficial del Estado, 12 de noviembre de 2020, núm.298.
- Real Decreto 319/1982, de 12 de febrero, por el que se reestructura y adscribe directamente el Servicio de Vigilancia Aduanera. Boletín Oficial del Estado, 25 de febrero de 1982, núm.48.
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado, 17 de septiembre de 1882, núm.260.

- Decreto de 2 de junio de 1944 por el que se aprueba con carácter definitivo el Reglamento de la organización y régimen del Notariado. Boletín Oficial del Estado,7 de julio de 1944, núm. 189.

JURISPRUDENCIA

Tribunal Constitucional:

- Sentencia 204/2016, de 10 de marzo.

Tribunal Supremo:

- Sentencia 179/2006 (Sala de lo Penal), de 14 de febrero.
- Sentencia 1281/2006 (Sala de lo Penal), de 27 de diciembre.
- Sentencia 104/2011 (Sala segunda, de lo Penal), de 1 de marzo.
- Sentencia 845/2014 (Sala segunda, de lo Penal), de 2 diciembre.
- Sentencia 97/2015 (Sala segunda, de lo Penal), de 24 de febrero.
- Sentencia 2047/2015 (Sala de lo Penal), de 19 de mayo.
- Sentencia 692/2017 (Sala de lo Penal), de 22 de febrero.
- Sentencia 324/2017 (Sala segunda, de lo Penal), de 8 de mayo.
- Sentencia 2949/2018 (Sala de lo Penal), del 19 de julio.
- Sentencia 591/2018 (Sala Segunda, de lo Penal) de 26 de noviembre.
- Sentencia 140/2019 (Sala de lo Penal) de 13 de marzo.